Unterricht in Kryptologie

Monika Stohr

Dissertation
an der Fakultät für Mathematik, Informatik und Statistik
der Ludwig–Maximilians–Universität München

München, 27. September 2007

Lehrstuhl für Didaktik der Mathematik

Unterricht in Kryptologie

Monika Stohr

Vollständiger Abdruck der von der Fakultät für Mathematik, Informatik und Statistik der Ludwig–Maximilians–Universität München zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften (Dr. rer. nat.)

genehmigten Dissertation.

Erster Berichterstatter:	Prof. Dr. F. Rudolf Fritsch
Zweiter Berichterstatter:	Prof. Dr. Albrecht Beutelspacher
Tag der Einreichung:	27. September 2007
Tag der mündlichen Prüfung:	02. Mai 2008

Danksagung

Mein besonderer Dank geht an Herrn Prof. Dr. Rudolf Fritsch, der mich zu dieser Arbeit ermutigt und sie mir ermöglicht hat. Bedanken möchte ich mich insbesondere für seine Betreuung und seine zahlreichen Ratschläge, die entscheidend zum Gelingen der Arbeit beigetragen haben.

Weiterhin danke ich der Schulleitung der Städtischen Elly–Heuss–Realschule in München für das Vertrauen, das sie mir entgegen gebracht hat. Besonderer Dank gilt dem Schulleiter Herrn Klaus Fertmann, der sich für mich eingesetzt und es mir ermöglicht hat, einen Wahlunterricht Kryptologie anzubieten und durchzuführen.

Ohne den Rückhalt meines Ehemannes wäre diese Arbeit nicht entstanden. Bedanken möchte ich mich deshalb bei Jürgen, der den Weg der Promotion vor mir gegangen ist, sein Wissen und seine Erfahrung mit mir geteilt hat und mich immer wieder mit aufmunternden Worten unterstützt hat.

Für Jürgen

Inhaltsverzeichnis

Kurzfassung

Kryptologie, die Wissenschaft von den Geheimschriften und ihrer Entschlüsselung, erfährt in der gegenwärtigen Zeit zunehmend praktische Bedeutung. Sie gewährleistet nicht nur Vertraulichkeit, Integrität und Authentizität beim Nachrichtenaustausch, sondern bestimmt auch die Sicherheit des elektronischen Geschäftsverkehrs, des Datenschutzes und ermöglicht digitale Signaturen. Gleichzeitig stützen sich moderne Verfahren der Kryptologie auf die Zahlentheorie, deren Grundlagen bereits in der Sekundarstufe I bereitgestellt werden. In der Vereinigung von mathematischen Inhalten, historischen Entwicklungen und aktuellen gesellschaftspolitischen Aspekten bietet Kryptologie vielfältige Einsatzmöglichkeiten für den Unterricht an allgemeinbildenden Schulen. Dass kryptologische Inhalte dennoch nicht in den Schulunterricht integriert sind, ist Anlass dieser Arbeit.

Ausgehend vom Bildungs- und Erziehungsauftrag allgemeinbildender Schulen wird zunächst die Berechtigung eines Unterrichts in Kryptologie nachgewiesen. Anschließend wird dessen didaktischer Ort festgelegt, es werden geeignete Lerninhalte ausgewählt und in eine zeitliche Abfolge gebracht. In einer Unterrichtssequenz werden diese kryptologischen Lerninhalte didaktisch aufbereitet, auf Verständnisebene der Schüler transferiert und mit methodischen Hinweisen für Lehrkräfte versehen.

Abstract

Cryptology is the science of ciphers and their decoding, which gains importance in recent years. It ensures privacy, integrity and authenticity of messages. Cryptology affects the security of electronic business connections and ensures security of data. In addition, cryptology makes digital signatures possible. At the same time modern procedures of cryptology rely on number theory, whose basic principles are provided in the "Sekundarstufe I". The combination of mathematical contents, history of humanity, and current socio-political aspects offers a lot of possible applications to a subject cryptology at general-education schools. However, cryptological contents are not integrated in instruction so far, which is the motivation of this thesis.

At first, this thesis proves the eligibility of an instruction in cryptology with the education mandate and the responsibility for education of general-education schools. Subsequently, the didactical place of this subject is specified, and the learning content is selected and scheduled. The cryptological knowledge is prepared didactically in a sequence of lessons, with regard to the understanding level of pupils and with methodical notes for instructors.

1 Einleitung

1.1 Motivation

Obwohl Kryptologie, die Wissenschaft von den Geheimschriften und ihrer unbefugten Entzifferung, eine jahrtausende alte Vergangenheit aufweist, ist ihre Bedeutung in der Gegenwart größer als jemals zuvor. Sie bestimmt die Absicherung weltweiter Computernetze, den Schutz geheimer Daten, ermöglicht digitale Signaturen und elektronischen Geschäftsverkehr und liefert Verfahren zur Gewährleistung von Vertraulichkeit, Integrität und Authentizität beim Nachrichtenaustausch. Die gegenwärtigen technischen Fortschritte und die Entwicklung zum Informationszeitalter lassen vermuten, dass die Bedeutung der Kryptologie in den kommenden Jahren noch zunehmen wird.

Gleichzeitig stützen sich moderne Verfahren der Kryptologie auf die Zahlentheorie, deren Grundlagen bereits in der Sekundarstufe I an allgemeinbildenden Schulen bereitgestellt werden. Auch ältere kryptologische Verfahren setzen nur geringes mathematisches und abstraktes Denkvermögen voraus, wie es von Schülern der Mittelstufe beherrscht wird.

Der mathematische Gehalt kryptologischer Themen eignet sich für zahlreiche Unterrichtssequenzen in Mathematik und bietet sinnvolle Einsatzmöglichkeiten der Computer im Schulunterricht. Man erkennt, welchen Beitrag Mathematik zur Lösung praktischer gesellschaftlicher Probleme leisten kann. Daneben ermöglicht die gegenwärtige Bedeutung der Kryptologie die Thematisierung aktueller gesellschaftspolitischer Entwicklungen, wie sie z. B. in den Unterrichtsfächern Wirtschaftlehre bzw. Politik diskutiert werden. Die lange historische Entwicklung der Kryptologie spricht auch geschichtliche Ereignisse an, deren Verlauf durch diese Wissenschaft beeinflusst wurden und die zu den Lerninhalten des Unterrichtsfaches Geschichte zählen. Außerdem inspirieren Geheimschriften viele Autoren, so dass sich Kryptologie auch in der Literatur wiederfindet und im Deutschunterricht thematisiert werden kann.

Zu diesen positiven Einsatzmöglichkeiten kryptologischer Gegenstände in verschiedenen Unterrichtsfächern kommt ein starkes Interesse der Schüler von Unter- und Mittelstufe an Geheimschriften und ihrer Entschlüsselung hinzu. Daneben motiviert auch die praktische Bedeutung der Kryptologie die Schüler, sich mit diesem Thema auseinander zu setzen.

Dass trotz der großen gegenwärtigen Bedeutung, den vielfältigen schulischen Einsatzmöglichkeiten und des ansprechenden Charakters, Kryptologie nicht in den Unterricht der allgemeinbildenden Schulen integriert ist, wurde zum Anlass dieser Arbeit genommen.

Ausgehend von der Bedeutung dieser Wissenschaft in Zusammenhang mit dem Fehlen schulischer Ausbildung, wird zunächst die Berechtigung eines Unterrichts in Kryptologie nachgewie-

sen. Nach Herausarbeitung der für das Verständnis kryptologischer Themenbereiche notwendigen Vorkenntnisse, wird der didaktische Ort festgelegt. Anschließend werden kryptologische Lerninhalte ausgewählt, in eine zeitliche Abfolge gebracht und für den Schulunterricht aufbereitet.

1.2 Ziele dieser Arbeit

In dieser Arbeit wird ausgehend von der großen gegenwärtigen Bedeutung der Kryptologie eine mangelnde schulische Ausbildung in diesem Bereich festgestellt. Darüber hinaus wird aufgezeigt, dass sich mit kryptologischen Themen fächerübergreifendes Unterrichten verwirklichen lässt, dass geschichtliche Ereignisse aus einer neuen Perspektive betrachtet werden können und dass sich vielfältige Einsatzmöglichkeiten der Computer bieten. Ausgehend von dem Spannungsverhältnis zwischen praktischer Notwendigkeit, den positiven unterrichtlichen Aspekten und dem Fehlen eines Unterrichts in Kryptologie, wird die Berechtigung dieses Unterrichts nachgewiesen.

Ziel dieser Arbeit ist es, auf Grundlage des Bildungs- und Erziehungsauftrags der Schulen, einen Unterricht in Kryptologie vorzustellen, der einerseits zur Allgemeinbildung beiträgt und andererseits auf das Interesse und die Verständnisebene der Schüler zurechtgeschnitten ist. Hierzu ist ein Wahlunterricht in Kryptologie am Ende der Sekundarstufe I vorgesehen. Für diesen werden Lerninhalte ausgewählt, eine zeitliche Struktur festgelegt und Hinweise zu fächerübergreifenden Themen gegeben.

Um dem Anspruch der Allgemeinbildung genüge zu tun, sind für einen Unterricht Kryptologie sowohl frühe Ver- und Entschlüsselungsmethoden als auch moderne kryptologische Verfahren vorgesehen. In einer beispielhaften Unterrichtssequenz werden diese kryptologischen Themen didaktisch auf die Verständnisebene der Schüler reduziert und so aufbereitet, dass zuvor festgelegte Lernziele erreicht werden können. Daneben werden Möglichkeiten der unterrichtlichen Vermittlung aufgezeigt, sowie Hinweise zu Computereinsätzen und methodischen Entscheidungen gegeben.

1.3 Gliederung

Die vorliegende Arbeit ist wie folgt gegliedert: In Kapitel 2 werden Grundlagen zu Ver- und Entschlüsselungsmethoden erläutert, die einem besseren Verständnis dieser Arbeit dienen. Das darauffolgende Kapitel 3 beschäftigt sich mit der Bedeutung der Kryptologie im Alltag und Unterricht und stellt fächerübergreifende Aspekte der Kryptologie vor. In Kapitel 4 werden verwandte Arbeiten zur Kryptologie vorgestellt, um eine Abgrenzung zur vorliegenden Arbeit zu erreichen. Ausgehend vom Bildungs- und Erziehungsauftrag allgemeinbildender Schulen erfährt ein Unterricht in Kryptologie in Kapitel 5 seine Berechtigung. Außerdem wird der didaktische Ort festgelegt, Lerninhalte bestimmt und in eine zeitliche Abfolge gebracht. In Kapitel 6

wird eine Unterrichtssequenz in Kryptologie vorgestellt, wobei vor allem Inhalte und Intentionen dargelegt und didaktisch für den Schulunterricht aufbereitet werden. Diese Unterrichtssequenz wurde im Schuljahr 2006/2007 an der Städtischen Elly–Heuss–Realschule in München in einem Wahlunterricht Kryptologie praktisch durchgeführt. Erkenntnisse aus diesem Unterricht sind im Kapitel 7 dargelegt.

2 Grundlagen

Kryptographie ist die Wissenschaft von der Verschlüsselung von Daten und der Entwicklung von Verschlüsselungsverfahren. *Kryptanalyse* – auch *Kryptoanalyse* genannt – ist die Wissenschaft von der Entschlüsselung von Daten ohne Kenntnis des Schlüssels. Durch diese Analysen lässt sich die Sicherheit kryptographischer Verfahren beurteilen. Beide Wissenschaften zusammen – Kryptographie und Kryptanalyse – bilden die *Kryptologie*. Als Kryptologie wird folglich "die Lehre von den Geheimschriften und ihrer unbefugten Entzifferung"[1)] bezeichnet.

Die *Steganographie* ist eine zur Kryptographie verwandte Wissenschaft. Ihr Ziel ist das Verbergen einer Nachricht und deren versteckte Übermittlung. Man spricht hier auch von den "verdeckten" Geheimschriften. Dem gegenüber spricht man bei der Kryptographie von den "offenen" Geheimschriften da sie beabsichtigt, Nachrichten für einen unbefugten Dritten unleserlich zu machen ohne deren Existenz zu verbergen.

2.1 Grundlagen der Kryptographie

Eine unverschlüsselte Nachricht bezeichnet man als *Klartext*. Die Ver- und Entschlüsselung einer Nachricht erfolgt auf Grundlage eines *Schlüssels*, durch den sowohl eine Verschlüsselungsfunktion als auch eine Entschlüsselungsfunktion festgelegt wird. Die verschlüsselte Nachricht wird *Geheimtext* oder *Kryptogramm* genannt. Das Verschlüsseln einer Nachricht bezeichnet man auch als *Chiffrieren* und das Entschlüsseln wird entsprechend *Dechiffrieren* genannt.

Die Verfahren der Kryptographie können in grundsätzlich zwei Bereiche eingeteilt werden: in die *symmetrischen* und die *asymmetrischen* Verfahren.

2.1.1 Symmetrische Chiffrierverfahren

Die Geschichte der Kryptographie beginnt mit den symmetrischen Chiffrierverfahren, die zahlreiche Verschlüsselungsarten beinhalten (vgl. Abbildung 2.1).

[1)] [2], S. 2

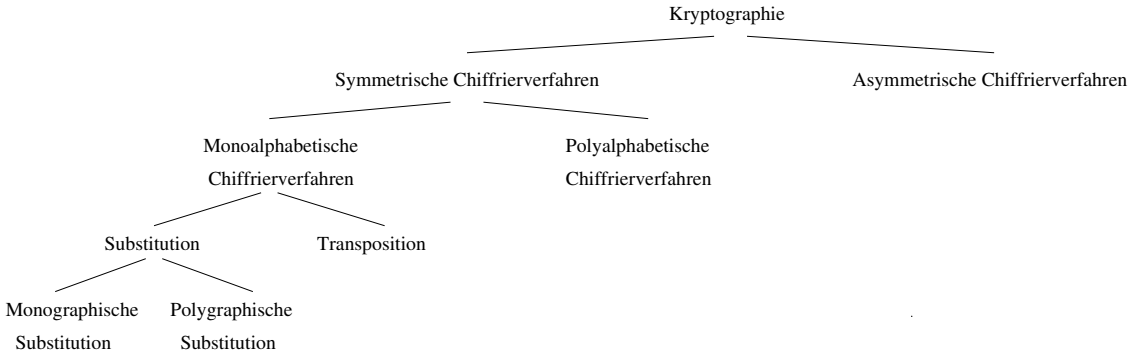


Abbildung 2.1: Einteilung der Kryptographie

2.1.1.1 Monoalphabetische Chiffrierverfahren

Die bis zum 16. Jahrhundert vorherrschenden kryptographischen Verfahren werden als *monoalphabetische Chiffrierverfahren* bezeichnet. Gekennzeichnet sind diese Chiffren dadurch, dass derselbe Chiffrierschritt wiederholt angewandt wird.

Monographische Substitution
Das älteste Beispiel monoalphabetischer Verfahren ist die Caesar–Chiffre. Caesar wird zugeschrieben, dass er Nachrichten verschlüsselte, indem er jeden Buchstaben um drei Stellen im Alphabet nach links versetzte (vgl. Abbildung 2.2).

Klartextalphabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	↓																									
Geheimtextalphabet:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Abbildung 2.2: Caesar–Chiffre

Verschlüsselt wird, indem jeder Buchstabe des Klartextes durch den darunter stehenden Buchstaben ersetzt wird. Zum Entschlüsseln werden die Geheimtextzeichen durch den entsprechenden darüber stehenden Buchstaben ersetzt. Der Schlüssel (s) dieser Chiffre ist die Anzahl der Stellen, um die das Alphabet nach links verschoben wird.

Identifiziert man die 26 Buchstaben des Alphabets mit den ganzen Zahlen von 0 bis 25, ergibt sich als Verschlüsselungsfunktion V: $V(k) = (k + s) \bmod 26$. Analog lautet die Entschlüsselungsfunktion E: $E(c) = (c - s) \bmod 26$.

Da bei der Caesar–Chiffre das Geheimtextalphabet durch Verschieben des Klartextalphabets hervorgeht, spricht man auch von einer *Verschiebechiffre*. Die Verschiebechiffre ist ein Spezialfall der *monographischen Substitution*. Bei dieser Verschlüsselung werden einzelne Klartextzeichen stets durch dieselben Geheimtextzeichen ersetzt. Im Allgemeinen wird dabei die alphabetische Reihenfolge nicht beibehalten.

Das Problem bei diesen Chiffren besteht darin, sich die Zuordnung der Zeichen zu merken. Erleichtert wird dies, indem man Geheimtextalphabete konstruiert, die aus einem Schlüsselwort hervorgehen. Dazu wird ein Schlüsselwort ohne Buchstabenwiederholungen unter einen

Klartextalphabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Geheimtextalphabet:	P	Q	R	T	U	V	W	X	Y	Z	G	E	H	I	M	N	S	A	B	C	D	F	J	K	L	O

Abbildung 2.3: Einzelzeichen werden durch Einzelzeichen ersetzt

Schlüsselbuchstaben des Klartextalphabets geschrieben. Anschließend werden die restlichen Buchstaben des Alphabets der Reihe nach aufgelistet. Im obigen Beispiel (vgl. Abbildung 2.3) geht das Geheimtextalphabet aus dem Schlüsselwort “Geheimnis” und dem Schlüsselzeichen “K” hervor.

Neben dem Ersetzen von Klartextbuchstaben durch einzelne Geheimtextzeichen, können Klartextzeichen auch durch mehrere Geheimtextzeichen ersetzt werden, wie Abbildung 2.4 zeigt.

Klartextalphabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Geheimtextalphabet:	01	86	02	63	22	06	54	42	28	66	19	84	26	60	04	38	12	43	44	87	68	20	55	07	21	14	64
	59				67				75					71													48
					18																					

Abbildung 2.4: Einzelzeichen werden durch mehrere Geheimtextzeichen ersetzt

Beim Verschlüsseln ersetzt man die Klartextzeichen zufällig durch ein darunter stehendes Geheimtextzeichen. Ziel dieser Chiffrierung ist, die Buchstabenhäufigkeiten zu verschleiern, da diese den Ansatzpunkt der Kryptanalyse darstellen (siehe Seite 12). An obigem Beispiel zeigt sich auch, dass das Geheimtextalphabet nicht aus Buchstaben bestehen muss, sondern vielmehr beliebige Zeichen enthalten kann. Da den beiden Zahlen 64 und 48 kein Klartextzeichen entspricht, bezeichnet man diese als Blender. Sie können im Geheimtext willkürlich eingebaut werden und dienen zur Täuschung des unbefugten Dechiffrierers.

Polygraphische Substitution
Im Gegensatz zur monographischen Substitution, bei der nacheinander einzelne Klartextzeichen verschlüsselt werden, werden bei der *polygraphischen Substitution* in einem Schritt mehrere Klartextbuchstaben chiffriert.

Die gleichzeitige Verschlüsselung von zwei Klartextzeichen bezeichnet man als Bigramm–Substitution. Die ältesten Bigramm–Substitutionen von Bedeutung sind das vom britischen Physiker Charles Wheatstone entwickelte und 1854 von seinem Freund Baron Playfair von St. Andrews veröffentlichte Playfair–Verfahren sowie das 1901 vorgestellte Verfahren des durch sein Werk “Traité Élémentaire der Cryptographie” berühmt gewordenen Franzosen Félix M. Delastelle.

- Bei der Playfair–Verschlüsselung wird ein aus einem Schlüsselwort (PALMERSTONE) hergeleitetes Alphabet (ohne dem Buchstaben J) in ein Quadrat geschrieben (vgl. Abbildung 2.5).

  In einem Schritt werden zwei Klartextzeichen nach folgendem Schema ersetzt:

P	A	L	M	E
R	S	T	O	N
B	C	D	F	G
H	I	K	Q	U
V	W	X	Y	Z

Abbildung 2.5: Playfair–Verfahren

- Stehen beide Klartextzeichen in einer Zeile, werden sie jeweils durch den rechten Nachbarn ersetzt; z. B. wird “SO” durch “TN” verschlüsselt.
- Stehen beide Klartextzeichen in einer Spalte, werden sie jeweils durch den darunter stehenden Buchstaben ersetzt; z. B. wird “TK” durch “DX” chiffriert.
- Stehen beide Klartextzeichen in verschiedenen Zeilen und Spalten, so werden sie durch den in derselben Zeile, aber in der Spalte des jeweils anderen Klartextzeichens stehenden Buchstaben ersetzt. So wird z. B. das Buchstabenpaar “SU” durch “NI” ersetzt.
- Doppelte Zeichen werden durch den Einschub von x vermieden.

- Beim Verfahren von Delastelle wird ebenfalls ein aus einem Schlüsselwort (BORDEAUX) gewonnenes Alphabet (ohne dem Buchstaben W) in ein Quadrat geschrieben, das als eine 5 x 5 Matrix aufgefasst wird (vgl. Abbildung 2.6).

B	O	R	D	E
A	U	X	C	F
G	H	I	J	K
L	M	N	P	Q
S	T	V	Y	Z

Abbildung 2.6: Verfahren nach Delastelle

Die Bigramm–Substitution erfolgt nach folgendem Verfahren:

- Zu einem Klartextzeichenpaar werden die Zeilen- und Spaltenkoordinaten in dieser Matrix bestimmt. Zum Beispiel gehören zum Buchstabenpaar “AN” die Koordinaten (2,1) und (4,3).
- Die Spaltenkoordinate des ersten Zeichens wird mit der Zeilenkoordinate des zweiten Zeichens vertauscht. Im obigen Beispiel erhält man dadurch die Koordinaten (2,4) und (1,3).
- Die durch diese Koordinaten festgelegten Buchstaben werden als Geheimtextzeichen gewählt. Im Beispiel bildet das Buchstabenpaar “CR” das Geheimtextzeichen.

Neben der Bigramm–Substitution gehören auch Trigramm–Substitutionen – bei denen drei Klartextzeichen in einem Schritt ersetzt werden – und Codes zur polygraphischen Substitution. Bei Codes werden für Wörter, Satzteile oder ganze Sätze, Chiffren definiert und in einem Codebuch festgehalten.

Die bedeutungsvollste monoalphabetische, polygraphische Substitution ist der 1977 standardisierte DES (Data Encryption Standard), der auch heute noch von Banken erfolgreich eingesetzt wird. Diese Chiffre verschlüsselt Bitfolgen fester Verarbeitungslänge (64 Bits) und wird deshalb auch als *Blockchiffrierverfahren* bezeichnet. Über die Entstehungsgeschichte, Funktionsweise und Betriebsmodi des DES sei auf die Literatur[2)] verwiesen. Im Jahr 2002 wurde in den USA der DES vom AES (Advanced Encryption Standard) abgelöst.

Transposition
Die beschriebenen Chiffrierverfahren der monographischen und polygraphischen Substitution haben gemeinsam, dass Klartextzeichen durch Geheimtextzeichen ersetzt werden. Bei den Transpositionen werden die Klartextbuchstaben nicht ersetzt, sondern sie verändern ihre Position im Text. Ein einfaches Verfahren der Transposition ist z. B., wenn eine Nachricht in ein Rechteck zeilenweise eingeschrieben und spaltenweise ausgelesen wird (vgl. Abbildung 2.7).

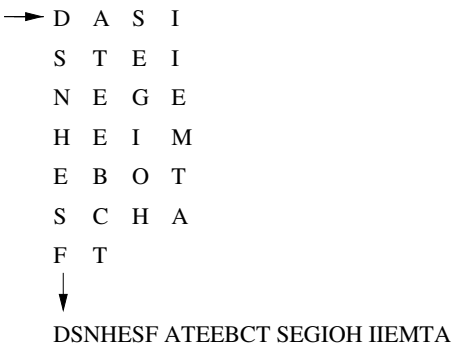


Abbildung 2.7: Einfache Transposition

Variationen dieser Transposition vertauschen vor dem Auslesen der Nachricht die Zeilen bzw. Spalten. Der Schlüssel zu dieser Chiffre ist die Anzahl der Spalten.

2.1.1.2 Polyalphabetische Chiffrierverfahren

Den bisher dargelegten kryptographischen Verfahren ist gemeinsam, dass derselbe Chiffrierschritt wiederholt angewandt wird. Demgegenüber findet bei den *polyalphabetischen Verfahren* ein Wechsel der Chiffrierschritte statt. Das bekannteste polyalphabetische Chiffrierverfahren veröffentlichte 1586 der französische Diplomat und Kryptograph Blaise de Vigenère.

Vigenère–Verschlüsselung
Zur Vigenère–Verschlüsselung verwendet man ein Schlüsselwort und das aus 26 verschobenen Alphabeten bestehende Vigenère–Quadrat (vgl. Abbildung 2.8).

[2)] z. B. [10], [16]

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Abbildung 2.8: Vigenère–Quadrat

Zur Verschlüsselung schreibt man das Schlüsselwort zeichenweise unter den Klartext und zwar so oft, bis die Länge der Nachricht erreicht ist. Der Buchstabe des Schlüsselwortes unter einem Klartextbuchstaben gibt nun an, mit welchem der verschobenen Alphabete die Verschiebechiffre angewandt wird: der Klartextbuchstabe wird mit dem Alphabet verschlüsselt, bei dem der Schlüsselwortbuchstabe in der 1. Spalte des Vigenère–Quadrats steht.

Vernam–Verschlüsselung
Ebenfalls zu den polyalphabetischen Chiffrierverfahren gehört das 1917 als “one–time pad” bekannt gewordene Verschlüsselungsverfahren von Gilbert S. Vernam, einem amerikanischen Ingenieur der Telefon- und Telegrafengesellschaft AT&T. Grundlage dieser Chiffre ist ein fortlaufender, nur einmal zu verwendender Schlüssel in Form einer Folge von Schlüsselzeichen. Der Klartext wird ebenfalls als Folge von Buchstaben aufgefasst (vgl. Abbildung 2.9).

Die Verschlüsselung erfolgt dadurch, dass die 26 Buchstaben des Alphabets mit den ganzen Zahlen von 0 bis 25 interpretiert werden und der i-te Klartextbuchstabe mit dem i-ten Schlüsselbuchstaben addiert wird (modulo 26). Damit ergibt sich als Verschlüsselungsfunktion V: $V(k_i) = (k_i + s_i) \bmod 26$ und als Entschlüsselungsfunktion E: $E(c_i) = (c_i - s_i) \bmod 26$.

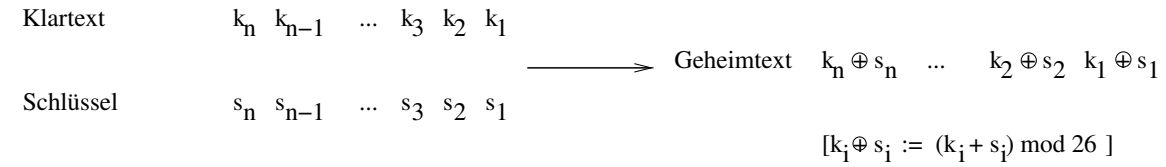


Abbildung 2.9: Verschlüsselung mit dem one–time pad

Diese auch als (additive) Stromchiffrierung bezeichnete Verschlüsselung wird vor allem mit Bits betrieben. In diesem Fall erhält man den Geheimtext durch binäre Addition.

Werden die einzelnen Schlüsselzeichen zufällig mit gleicher Wahrscheinlichkeit gewählt und wird der Schlüssel nur einmal verwendet, ist diese Chiffre für einen unbefugten Dritten nicht zu knacken. Man spricht in diesem Fall von theoretischer oder perfekter Sicherheit.

2.1.2 Asymmetrische Chiffrierverfahren

Symmetrische Chiffrierverfahren sind dadurch gekennzeichnet, dass zum Ver- und Entschlüsseln derselbe Schlüssel verwendet wird, der zuvor zwischen den Kommunikationspartnern auf einem sicheren Weg ausgetauscht werden muss. Gerade diesen Nachteil des Schlüsselaustauschs will man bei asymmetrischen Chiffrierverfahren – auch *Public–Key–Verfahren* genannt – vermeiden. Dazu wird ein Schlüsselpaar, bestehend aus einem öffentlichen Schlüssel und einem privaten Schlüssel, erzeugt. Nachrichten werden dann mit dem frei verfügbaren öffentlichen Schlüssel chiffriert und an den Empfänger geschickt. Dieser entschlüsselt den Geheimtext mit Hilfe des privaten Schlüssels, der geheim gehalten werden muss.

RSA
Das bekannteste asymmetrische Chiffrierverfahren ist das 1978 von Ronald L. Rivest, Adi Shamir und Leonard M. Adleman veröffentlichte RSA–Verfahren. Bei diesem werden zwei (verschiedene) große Primzahlen p und q gewählt. Anschließend berechnet man

$$n = p \cdot q$$

und die Eulersche ϕ–Funktion

$$\phi(n) = (p-1) \cdot (q-1) \, .$$

Nun wählt man eine natürliche Zahl e, teilerfremd zu $\phi(n)$, mit $1 < e < \phi(n)$ und berechnet (z. B. mit Hilfe des erweiterten euklidischen Algorithmus) eine natürliche Zahl d mit $1 < d < \phi\,(n)$, so dass gilt:

$$e \cdot d \equiv 1 \bmod \phi(n) \, .$$

Die beiden Zahlen n und e werden öffentlich bekannt gegeben. Die Zahl d wird zum entschlüsseln verwendet und stellt den geheimen privaten Schlüssel dar. Natürlich müssen auch p, q und $\phi(n)$ geheim bleiben. Die Zahl n wird RSA–Modul genannt, die Zahl e heißt Verschlüsselungsexponent und die Zahl d Entschlüsselungsexponent.

Um eine Nachricht zu chiffrieren, muss diese zunächst in eine Zahl m (mit $0 \leq m < n$) verwandelt werden. Beispielsweise kann dazu ein Wort nach ASCII[3)] codiert und dessen Dezimalzahl verwendet werden. Nachdem der öffentliche Schlüssel besorgt wurde, berechnet der Sender den Geheimtext mit der Verschlüsselungsfunktion

$$V(m) = m^e \bmod n \, .$$

[3)] American Standard Code for Information Interchange

Die Entschlüsselung des Geheimtextes erfolgt durch

$$E(c) = c^d \bmod n \ .$$

Die Sicherheit des RSA–Verfahrens beruht im wesentlichen darauf, dass die Faktorisierung von n nicht möglich ist. Aus diesem Grund sollten die Primzahlen p und q so gewählt werden, dass n mindestens 512 Bits lang ist.

Da

$$(m^d)^e = (m^e)^d \equiv m \bmod n$$

gilt, sind die Ver- und Entschlüsselungsfunktion vertauschbar. Damit eignet sich das RSA–Verfahren neben der Verschlüsselung auch zum Signieren[4)] einer Nachricht.

Um eine Zahl m zu signieren, berechnet man die Signatur s mit $s = m^d \bmod n$. Zur Überprüfung der Signatur ist mit dem öffentlichen Schlüssel $s^e \bmod n$ zu berechnen. Ergibt sich daraus der Wert m, ist die Signatur verifiziert.

Diffie–Hellman–Schlüsselaustausch
Der von Whitfield Diffie und Martin E. Hellman entwickelte Diffie–Hellman–Schlüsselaustausch ist ein Verfahren, wie ein Schlüssel (einer symmetrischen Chiffre) über einen unsicheren Kanal vereinbart werden kann, ohne dass ein Zuhörer den Schlüssel in Erfahrung bringen kann. Es ist folglich kein Verschlüsselungsverfahren an sich, stellt aber die Grundlage für das ElGamal–Verfahren dar (siehe unten).

Beim Diffie–Hellman–Schlüsselaustausch müssen sich zwei Kommunikationspartner – Alice und Bob genannt – über eine Primzahl p und über eine Primitivwurzel $g \bmod p$ mit $1 < g < p-1$ einig sein. Diese Zahlen p und g können öffentlich bekannt sein.

Nun wählt Alice eine geheime natürliche Zahl a, mit $a < p - 1$ und berechnet

$$A = g^a \bmod p \ .$$

Auch Bob wählt eine geheim zu haltende natürliche Zahl b, mit $b < p - 1$ und berechnet

$$B = g^b \bmod p \ .$$

Anschließend schickt jeder sein Ergebnis dem anderen Kommunikationspartner. Alice berechnet nun

$$B^a \bmod p$$

und Bob berechnet analog

$$A^b \bmod p \ .$$

Da

$$B^a \bmod p = (g^b)^a \bmod p = (g^a)^b \bmod p = A^b \bmod p$$

[4)] Eine Signatur stellt eine elektronische Unterschrift dar und dient somit zur Authentifizierung der Kommunikationspartner.

ist, erhält jeder der beiden Kommunikationspartner das gleiche Ergebnis, das als Schlüssel verwendet wird.

ElGamal–Chiffrierverfahren
Beim Chiffrierverfahren nach Tahir ElGamal ist zur Schlüsselerzeugung zunächst eine Primzahl p und eine Primitivwurzel g mod p zu wählen. Danach wählt man zufällig eine natürliche Zahl a mit $1 < a < p - 1$ und berechnet

$$A = g^a \bmod p\,.$$

Die Zahlen p, g und A werden öffentlich bekannt gegeben. Die Zahl a ist der private Schlüssel eines Teilnehmers und muss geheim gehalten werden.

Um eine Nachricht zu verschlüsseln, ist diese (wie beim RSA–Verfahren) in eine Zahl m mit $0 \leq m < p$ zu überführen. Anschließend wählt der Sender der Nachricht zufällig eine natürliche Zahl b mit $1 \leq b < p - 1$ und berechnet

$$B = g^b \bmod p$$

und

$$c = A^b m \bmod p\,.$$

Das Zahlenpaar (B,c) stellt den Geheimtext dar und kann an den Empfänger geschickt werden.

Da nach dem kleinen Satz von Fermat die Gleichung $g^{p-1} \equiv 1 \bmod p$ erfüllt ist, gilt

$$B^{(p-1-a)}c \equiv g^{b(p-1-a)}A^b m \equiv (g^{p-1})^b (g^a)^{-b} A^b m \equiv A^{-b}A^b m \equiv m \bmod p\,.$$

Um den Geheimtext (B,c) zu entschlüsseln, berechnet der Empfänger folglich

$$B^{p-1-a}c \bmod p\,.$$

2.2 Grundlagen der Kryptanalyse

Neben der Verschlüsselung von Daten umfasst die Kryptologie auch die Kryptanalyse, die Wissenschaft vom unbefugten Entziffern chiffrierter Texte. Auf diese Weise kann die Sicherheit kryptographischer Verfahren beurteilt werden. Grundlage der Kryptanalyse bildet dabei das Prinzip von Kerckhoffs: Die Sicherheit eines kryptographischen Verfahrens darf nur auf der Geheimhaltung des Schlüssels beruhen und nicht auf der Geheimhaltung des Algorithmus. Man geht also grundsätzlich davon aus, dass ein unbefugter Angreifer das Verschlüsselungsverfahren kennt.

Um die Sicherheit verschlüsselter Texte beurteilen zu können, ist zu bestimmen, welche Angriffe auf den Geheimtext möglich sind.

Angriffsarten

- Ciphertext–Only–Attacke: Der Kryptoanalytiker kennt nur den Geheimtext. Dies ist der schwächste, aber auch der wahrscheinlichste Angriff, da der Geheimtext auf einem unsicheren Kanal verschickt wird und leicht abgefangen werden kann.
- Known–Plaintext–Attacke: Der Kryptoanalytiker kennt Klartexte mit den dazugehörigen Geheimtexten. Dieser Fall tritt z. B. bei verschlüsselten Briefen mit den allgemein bekannten Grußfloskeln ein.
- Chosen–Plaintext–Attacke: Der Kryptoanalytiker kann zu selbst gewählten Klartexten den Geheimtext erzeugen. Bei asymmetrischen Chiffrierverfahren ist dieser Angriff immer möglich, da der Schlüssel zum Chiffrieren öffentlich bekannt ist. Ein Beispiel aus dem Bereich der symmetrischen Verfahren stammt aus dem Zweiten Weltkrieg: Die Alliierten kannten die Texte, die von deutschen Schiffen bei Beobachtung einer Wasserbombe gesendet wurden. Um mittels einer Chosen–Plaintext–Attacke den Schlüssel von deutschen Geheimtexten zu finden, warfen die Alliierten Wasserbomben ab und fingen die gesendeten Chiffrate ab. Die Klartexte waren selbst gewählt, da Zeitpunkt und Ort bei Abwurf der Wasserbombe frei festgelegt werden konnten.[5)]
- Chosen–Ciphertext–Attacke: Der Kryptoanalytiker kann zu selbst gewählten Geheimtexten die Klartexte bestimmen, ohne den Schlüssel zu kennen.

Im Folgenden werden die bekanntesten Ciphertext–Only–Attacken zu verschiedenen kryptographischen Verfahren vorgestellt.

Systematisches Durchprobieren aller Schlüssel
Eine Möglichkeit, einen Geheimtext ohne Kenntnis des Schlüssels zu entziffern, besteht darin, sämtliche Schlüssel systematisch durch zu probieren. Man spricht hier von *Brute–Force–Attacken*. Diese Methode führt nur dann unter zumutbarem Aufwand zum Erfolg, wenn der Schlüsselraum des kryptographischen Verfahrens relativ klein ist. So gibt es z. B. bei der Verschiebechiffre nach Caesar nur 26 Möglichkeiten, die Klar- und Geheimtextalphabete anzuordnen. Der zeitliche Aufwand, alle möglichen Verschiebe–Schlüssel zu prüfen, ist sehr gering. Erleichtert wird die Suche nach dem richtigen Schlüssel dadurch, dass nicht der gesamte Geheimtext zur Schlüsselsuche herangezogen werden muss, sondern nur ein Teil davon. Man erkennt sehr schnell, ob es sich bei den erhaltenen Buchstabenkombinationen um sinnvolle Wörter handelt.

Die Möglichkeit, alle Schlüssel durch zu probieren, stößt jedoch schnell an ihre Grenzen. Wird die Reihenfolge des Alphabets bei der Verschlüsselung nicht eingehalten, gibt es 26! ($\approx 4 \cdot 10^{26}$) mögliche Anordnungen von Klar- und Geheimtextalphabeten. Für Geheimtexte, die durch monographische Verschlüsselungen hervorgegangen sind, hat sich deshalb die Analyse der Buchstabenhäufigkeit zur Entschlüsselung bewährt.

Analyse der Buchstabenhäufigkeit
In jeder natürlichen Sprache treten die Buchstaben unterschiedlich oft in Wörtern auf. Dies bedeutet, dass jeder Buchstabe eine charakteristische Häufigkeit in einer Sprache aufweist.

[5)] vgl. [10], S. 63

Aus unten stehender Tabelle[6] ist zu erkennen, dass der Buchstabe e in der deutschen Sprache am häufigsten auftritt, gefolgt von den Buchstaben n, i, s, r, a und t. Daneben gibt es Buchstaben, wie z. B. x und q, die nur sehr selten in einem Text vorkommen.

Um einen monoalphabetisch verschlüsselten Text zu entschlüsseln, werden nach dieser Methode die relativen Häufigkeiten der Geheimtextzeichen im betreffendem Chiffrat bestimmt. Durch Vergleich mit den Buchstabenhäufigkeiten der Klartextsprache erhält man einen Hinweis darauf, um welche Klartextzeichen es sich handeln könnte. So könnte das häufigste Geheimtextzeichen für den Buchstaben “E” , das zweithäufigste für den Buchstaben “N” stehen usw.

Häufigkeiten der Buchstaben in der deutschen Sprache

Buchstabe	Häufigkeit in %	Buchstabe	Häufigkeit in %
a	6,51	n	9,78
b	1,89	o	2,51
c	3,06	p	0,79
d	5,08	q	0,02
e	17,40	r	7,00
f	1,66	s	7,27
g	3,01	t	6,15
h	4,76	u	4,35
i	7,55	v	0,67
j	0,27	w	1,89
k	1,21	x	0,03
l	3,44	y	0,04
m	2,53	z	1,13

In einem weiteren Schritt zieht man die Häufigkeiten der Bigramme von Buchstaben heran. Diese helfen, vorhandene Vermutungen zu bekräftigen und weitere Klartextbuchstaben im Geheimtext zu erkennen[7].

Häufigkeiten der Bigramme in der deutschen Sprache

Bigramm	Häufigkeit in %	Bigramm	Häufigkeit in %
en	3,88	nd	1,99
er	3,75	ei	1,88
ch	2,75	ie	1,79
te	2,26	in	1,67
de	2,00	es	1,52

Durch diese Analysen können die häufigsten Klartextbuchstaben entziffert werden. Weitere Buchstaben lassen sich ab jetzt auch erraten. Durch probeweises Einsetzen der Vermutungen zeigt sich sehr schnell, ob die Annahme richtig war oder nicht. Sollten noch weitere Indizien benötigt werden, können auch die Häufigkeiten von Buchstaben–Trigrammen analysiert werden. Insbesondere bei langen Texten gelingt auf diese Weise das Entziffern relativ schnell.

[6] vgl. [8], S. 18
[7] vgl. [8], S. 25

Kryptanalyse bei polyalphabetischen Chiffren
Polyalphabetisch chiffrierte Texte galten in der Kryptologie lange Zeit als sichere Verschlüsselungsverfahren, bis der preußische Infanteriemajor und Kryptograph Friedrich W. Kasiski 1863 in seinem Buch "Die Geheimschriften und die Dechiffrierkunst" eine Methode zur Kryptanalyse der Vigenère–Chiffre publizierte. Ein zweites Verfahren zur Entschlüsselung von Vigenère–Chiffren wurde 1920 vom russisch–amerikanischen Kryptographen William F. Friedman veröffentlicht und wird weiter unten dargelegt. Ziel beider Entschlüsselungsmethoden ist es, die Länge des Schlüsselwortes zu bestimmen.

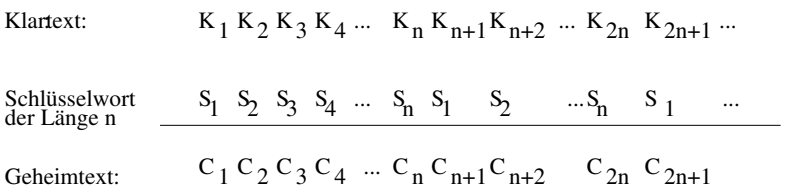


Abbildung 2.10: Vigenère–Verschlüsselung

Mit Hilfe der Schlüsselwortlänge n kann nach folgendem Schema dechiffriert werden:

- Wie Abbildung 2.10 zeigt, werden die Zeichen an den Positionen 1, n+1, 2n+1, 3n+1 usw. mit demselben Geheimtextalphabet verschlüsselt. Die Zeichen an den Positionen 2, n+2, 2n+2, 3n+2 usw. werden mit demselben Geheimtextalphabet verschlüsselt. Analog schließt man auf die weiteren Buchstaben des Chiffrates. Schließlich werden auch die Zeichen an den Positionen n, 2n, 3n usw. mit demselben Geheimtextalphabet chiffriert.

- Man selektiert die Geheimtextzeichen, die mit demselben Geheimtextalphabet verschlüsselt wurden. Auf diese Weise erhält man Texte, die nach einer einfachen Caesar–Verschiebechiffre verschlüsselt wurden. Diese Chiffrate sind einfach zu brechen und können zum Klartext zusammengesetzt werden.

Kasiski–Test
Der Kasiski–Test beruht auf der Annahme, dass Trigramme von Buchstaben oder bestimmte Wörter, in einem Text mehrmals auftreten. In der Regel werden diese unterschiedlich verschlüsselt. Ist aber der Abstand zwischen denselben Wörtern bzw. Trigrammen genau so groß oder ein Vielfaches der Schlüsselwortlänge, so werden diese Wörter gleich verschlüsselt.

Beim Kasiski–Test wird folglich ein Chiffrat nach Folgen gleicher Geheimtextzeichen untersucht. Der Abstand zwischen diesen Folgen ist die Länge des Schlüsselwortes oder ein Vielfaches von dieser. Erhält man unterschiedliche Abstandsgrößen zwischen gleichen Geheimtextzeichenfolgen, ist mit großer Wahrscheinlichkeit der größte gemeinsame Teiler der Abstandsgößen, die Länge des Schlüsselwortes.

Friedman–Test
Die von Friedman entwickelte Methode zur Kryptanalyse von Vigenère chiffrierten Texten wird auch als "Kappa–Test" bezeichnet. Grundlage dieses Entschlüsselungsverfahrens bildet der Koinzidenzindex κ. Der Koinzidenzindex gibt die relative Häufigkeit an, mit der zwei untereinan-

der liegende Texte zeichenweise übereinstimmen. Somit berechnet sich der Koinzidenzindex aus zwei gleich langen Texten $T = t_1 \dots t_M$ und $T' = t'_1 \dots t'_M$ wie folgt:

$$\kappa(T,T') := \frac{1}{M} \sum_{i=1}^{M} \delta(t_i, t'_i) \quad \text{mit} \quad \delta(t,t') = \begin{cases} 1 & falls \quad t = t' \\ 0 & falls \quad t \neq t' \end{cases}$$

Seien nun $T = t_1 \dots t_M$ und $T' = t'_1 \dots t'_M$ zwei Texte der Länge M über demselben N-elementigen Alphabet. Ferner seien Q und Q' stochastische Quellen über diesem Alphabet, die das j-te Zeichen mit der Wahrscheinlichkeit p_j bzw. p'_j ausgeben. Erfolgt die Generierung der Texte T und T' durch Q bzw. Q', erhält man als Erwartungswert für den Koinzidenzindex κ:

$$E(\kappa(T,T')) = \sum_{j=1}^{N} p_j p'_j.$$

Sind beide stochastische Quellen gleich, d. h. Q = Q', und die Texte T und T' unabhängig voneinander erzeugt, ergibt sich:

$$E(\kappa(T,T')) = \sum_{j=1}^{N} p_j^2.$$

Damit erhält man als Erwartungswert für κ für zufällig generierte Texte über dem Standardalphabet mit 26 Buchstaben:

$$E(\kappa(T,T')) = 26 \cdot \left(\frac{1}{26}\right)^2 = \frac{1}{26} \approx 0{,}03846.$$

Nachdem in natürlichen Sprachen die Buchstaben nicht gleichverteilt sind, sondern vielmehr bestimmte Häufigkeiten aufweisen, erhält man als Erwartungswert für κ für einen deutschsprachigen Text 0,07619 und für einen englischsprachigen Text 0,06577.

Eine kryptoanalytische Anwendung des Kappa–Tests besteht darin, dass sich die Häufigkeitsverteilung der Buchstaben bei einer monoalphabetischen Chiffrierung nicht ändert. Ein berechneter Wert für κ liegt folglich ungefähr beim Erwartungswert der jeweiligen Sprache. Bei polyalphabetischen Verschlüsselungsverfahren wird versucht, die Buchstabenhäufigkeiten aneinander anzupassen. Dadurch erhält man bei einer Berechnung von κ einen Wert, der deutlich unter dem Erwartungswert der Sprache liegt. Auf diese Weise lassen sich Chiffrate danach unterscheiden, ob sie durch monoalphabetische oder polyalphabetische Verfahren erzeugt wurden.

Das Verfahren von Friedman zur Bestimmung der Länge des Schlüsselwortes einer Vigenère chiffrierten Nachricht besteht darin, die Werte für κ des Geheimtextes C und des um u Positionen buchstabenweise nach rechts verschobenen Kryptogramms C^u zu berechnen. Die erhaltenen Werte werden dann in ein Diagramm eingetragen.

Wenn u ein Vielfaches der Schlüsselwortlänge ist, so ist ein Wert für κ in der Nähe des Erwartungswertes der Sprache zu erwarten, da alle untereinander stehenden Geheimtextzeichen jeweils nach derselben Caesar–Verschiebechiffre erzeugt wurden. Ist u jedoch kein Vielfaches

der Schlüssellänge, ist eine zeichenweise Übereinstimmung der Texte rein zufällig. Deshalb liegt hier der Wert für κ in der Nähe von 0,0385.

Nachdem die Werte für κ in ein Diagramm eingetragen wurden, lässt sich in diesem die Länge des Schlüsselwortes und die Vielfachen dieser Länge an den deutlich höheren Ergebnissen ablesen.

3 Bedeutung der Kryptologie

3.1 Kryptologie im Alltag

Obwohl Kryptologie eine jahrtausende alte Wissenschaft darstellt, ist ihre Bedeutung in unserer Gegenwart größer als jemals zuvor. Kryptologie ist nicht mehr länger eine Wissenschaft für Geheimdienste und Militär, sondern begegnet uns im alltäglichen Leben:

- Da digitale Bild- und Tonträger leicht und ohne Qualitätsverlust kopiert werden können, werden diese durch kryptologische Verfahren mit einem Kopierschutz versehen. Dieser wird durch das Digital Rights Management realisiert, das den Inhalt eines digitalen Trägers eindeutig an eine Lizenz bindet. Diese Lizenz enthält den Schlüssel, mit dem die Daten auf dem digitalen Bild- bzw. Tonträger lesbar gemacht werden können.

- E-Mails können sehr leicht abgefangen, gelesen und verändert werden. Auch Absender- und Empfängeradresse lassen sich leicht fälschen. Vertraulichkeit sowie Authentizität und Integrität der elektronischen Nachrichten kann durch Verschlüsselung erreicht werden. In diesem Bereich haben sich das von Phil Zimmermann entwickelte Verschlüsselungsprogramm PGP (Pretty Good Privacy) sowie die freie Verschlüsselungssoftware GnuPG (Gnu Privacy Guard) etabliert.

- Beim Online–Banking und bei Geldautomaten wird die persönliche Identifikationsnummer PIN (Personal Identification Number) mit dem kryptologischen Verfahren DES verifiziert.

- Bei Mobilfunknetzen und beim Pay–TV wird die berechtigte Benutzung durch kryptologische Verfahren sichergestellt. Bei Mobilfunknetzen dient hierzu die SIM–Karte (Subscriber Identity Module), die den Benutzer mittels einer veränderbaren PIN identifiziert. Beim Pay–TV wird mittels eines signierten Schlüssels auf einer Chipkarte (Dekoderkarte/Smartcard[1)]) das verschlüsselte Fernsehsignal entschlüsselt.

- Zum Schutz vor Trojanern werden Softwarepakete und Updates im Internet durch kryptologische Verfahren authentifiziert.

- Neben Sicherheit in Computernetzwerken kann durch die Verfahren der asymmetrischen Verschlüsselung, Verbindlichkeit beim Abschluss von Rechtsgeschäften im elektronischen Geschäftsverkehr (E–Commerce) erreicht werden.

[1)] Chipkarte, in die eine Hardware–Logik, Speicher oder ein Mikroprozessor eingebaut ist.

Außerdem konnte sich die auf kryptologischen Verfahren basierende elektronische Signatur in vielen Bereichen der Wirtschaft durchsetzen: “Fielmann und Metro akzeptieren nur noch digital signierte Rechnungen. Angebote für öffentliche Bauvorhaben werden im elektronischen Verfahren ohne händische Unterschrift abgegeben. Gerichte und Anwälte kommunizieren zunehmend elektronisch – signiert und häufig verschlüsselt. AOK und Lottogesellschaften setzen beim Datenaustausch ebenfalls auf die Smartcards. In diesen Fällen kommen bei den Behörden und Firmen Signier- und Verifizier–Server zum Einsatz, die große Mengen von Dokumenten ohne menschlichen Eingriff verarbeiten.”[2)]

Im Hinblick auf die Zukunft wird Kryptologie noch größere Bedeutung erlangen. So prognostiziert S. Singh in [30] dass “Volksabstimmungen in Demokratien auch per Online–Stimmabgabe möglich sein [werden], und der Staat wird sich das Internet für seine Aufgaben zunutze machen und den Bürgern beispielsweise die Möglichkeit bieten, ihre Steuererklärungen über das Netz abzuliefern. Für den Erfolg des Informationszeitalters ist jedoch wichtig, ob die Informationen auf ihrer Reise um den Globus geschützt werden können, und hier spielt die Kryptographie die entscheidende Rolle.”[3)]

3.2 Gegenwärtige schulische Ausbildung

Wie obige Beispiele zeigen, erlangt Kryptologie eine große praktische Bedeutung. Eine schulische Ausbildung in Kryptologie findet jedoch nur vereinzelt statt. Im Folgenden wird die Bedeutung der Kryptologie in den Bundesländern in Deutschland dargestellt, die kryptologische Inhalte im Lehrplan aufweisen.

Da Kryptologie eine Wissenschaft ist, die in zunehmenden Maße in der Informatik praktische Bedeutung erlangt, erfährt die Kryptologie am ehesten als Themengebiet im Informatikunterricht schulische Behandlung. Je nach Lehrplan wird die schulische Ausbildung in Kryptologie sehr unterschiedlich gehandhabt.

Kryptologie als verbindlicher Inhalt
In Bayern sieht der Lehrplan für die sechsstufige Realschule im Informatikunterricht der Jahrgangsstufe 9 (Wahlpflichtfächergruppe I) im Themengebiet “Historische, soziale und rechtliche Aspekte der EDV” ca. zwei Unterrichtsstunden für

- Schutz vor Datenmissbrauch
  (z.B. Verschlüsselung, digitale Signatur, Gesetze, Verhaltensregeln)[4)]

vor. Im Informatikunterricht des Gymnasiums und der Hauptschule ist Kryptologie als Themengebiet im Lehrplan nicht enthalten.

Im Saarland stellt die Einführung in “klassische kryptographische Verfahren” ein verbindliches Themengebiet im Informatikunterricht der gymnasialen Oberstufe mit 5 Unterrichtsstunden dar.

[2)] [21], S. 3
[3)] [30], S. 353
[4)] Bayerisches Staatsministerium für Unterricht und Kultus: Lehrplan für die sechsstufige Realschule, S. 485

Im Leistungskurs Informatik ist auch die Behandlung moderner kryptographischer Verfahren in 15 Unterrichtsstunden vorgesehen.[5)]

In Schleswig–Holstein wird im Fach Informatik in der Jahrgangsstufe 13/2 an Gymnasien, Gesamtschulen und Fachgymnasien "die Verflechtung der Informatik mit der Mathematik thematisiert". Unter den hierfür vorgeschlagenen Themen fallen folgende in das Fachgebiet der Kryptologie:

- ENIGMA
- Die richtige Karte ist der Schlüssel zur Welt
- Members only – Zugang nur mit Passwort
- Pay–TV ohne zu bezahlen?
- Soll jeder lesen, was ich schreibe?[6)]

Kryptologie als Wahlinhalt
In Berlin sieht der Rahmenplan für die Sekundarstufe I in der Doppeljahrgangsstufe 9/10 Kryptologie als Wahlthema im Mathematikunterricht des Wahlpflichtkurses I vor. Unter den Leitideen Zahl, Daten, Zufall sind Schwerpunkte des Themengebietes:

- Erkennen der gesellschaftlichen Relevanz der Thematik
- Einschätzen der Sicherheit verschiedener Verschlüsselungsverfahren
- Nutzen kombinatorischer Überlegungen zur Verschlüsselung
- Begründen der Notwendigkeit moderner kryptologischer Verfahren[7)]

Kryptologie als Wahlthema ist auch im Rahmenplan des Wahlpflichtfaches Informatik für die Jahrgangsstufen 8/9 des achtjährigen Gymnasiums in Hamburg vorgesehen. Schwerpunkte liegen hier in der Behandlung klassischer Verschlüsselungsverfahren; von modernen Chiffrierverfahren wird lediglich das Prinzip dargestellt.[8)]

Beim Hochbegabten Modell Mittelfranken – einem Projekt zur Förderung besonders begabter Schülerinnen und Schüler der 9. bis 11. Gymnasialklassen aus dem Raum Nürnberg, Fürth, Erlangen – wird u. a. ein Kurs in Kryptologie angeboten[9)]. Bei diesem, auf 6 bis 8 Doppelstunden beschränkten Kurs, liegt der Schwerpunkt deutlich auf den zahlentheoretischen Grundlagen beim RSA–Verfahren. Auf die klassische Kryptologie wird kaum eingegangen. Elektronische Unterschriften werden je nach zeitlichem Vorankommen ebenfalls aus mathematischer Sicht behandelt.

[5)] vgl. Ministerium für Bildung, Kultur und Wissenschaft: Achtjähriges Gymnasium – Informatik, S. III/IV
[6)] vgl. Ministerium für Bildung, Wissenschaft, Forschung und Kultur des Landes Schleswig–Holstein: Lehrplan für die Sekundarstufe II, S. 38
[7)] Senatsverwaltung für Bildung, Jugend und Sport: Rahmenplan für die Sekundarstufe I – Wahlpflichtkurs I, S. 30
[8)] vgl. Behörde für Bildung und Sport: Bildungsplan Achtstufiges Gymnasium Sekundarstufe I – Rahmenplan Wahlpflichtfach Informatik, S. 14
[9)] vgl. http://hochbegabung.gym-mfr.de

Eine weitreichende schulische Behandlung der Kryptologie ist in Sachsen–Anhalt möglich. Hier stellt Kryptologie eines unter acht Wahlthemen des Informatikunterrichts an Gymnasien im Kurshalbjahr 12/1 dar. In den Rahmenrichtlinien von Sachsen–Anhalt sind folgende Lernziele vorgesehenen:
"Die Schülerinnen und Schüler

- kennen Beispiele aus der historischen Entwicklung und wissen um die modernen gesellschaftlichen Aspekte der Kryptologie,
- kennen wesentliche Aufgaben der Kryptologie in der Vergangenheit und Gegenwart,
- kennen verschiedene Verfahren der Kryptographie und der Kryptoanalyse und können diese implementieren,
- kennen Vor- und Nachteile ausgewählter Chiffrierverfahren,
- können Klartexte in der gewählten Programmiersprache nach verschiedenen Algorithmen chiffrieren,
- können fremde, verschlüsselte Texte analysieren und in der verwendeten Programmiersprache dechiffrieren"[10)].

Für das mit 26 Unterrichtsstunden angesetzte Wahlthema "Kryptologie" stellt Jörn Zuber in [37] eine Unterrichtssequenz vor (siehe Seite 26).

Zusammenfassend gilt somit, dass Kryptologie als verbindlicher Lehrplaninhalt in lediglich drei Bundesländern (Bayern, Saarland, Schleswig–Holstein) schulische Behandlung erfährt. Allerdings ist die Anzahl der Unterrichtsstunden so gering, dass eine fundierte Ausbildung hierin nicht möglich ist. Daneben findet Kryptologie als Wahlinhalt in Berlin und Hamburg Eingang in den Unterricht, wobei die Schwerpunktsetzung auf den klassischen Verfahren beruht. Eine systematische und fundierte Behandlung kryptologischer Verfahren ist nur in Sachsen–Anhalt möglich. Doch aufgrund der Tatsache, dass Kryptologie eines unter acht Wahlthemen darstellt, verliert diese Wissenschaft auch hier an Bedeutung.

3.3 Fächerübergreifende Aspekte der Kryptologie

Wird die Kryptologie im Unterricht behandelt, ergeben sich zahlreiche Verbindungen zu anderen Unterrichtsfächern.

Mathematik
Kryptologie ist eine Wissenschaft, die zahlreiche mathematische Inhalte umfasst. So beruht bereits bei der Behandlung früher kryptologischer Verfahren die Kryptanalyse auf statistischen Methoden. Auch bei späteren Chiffrierverfahren ist die Kryptanalyse mathematisch geprägt, wobei insbesondere der Mathematiker William F. Friedman 1920 mit dem "Friedman–Test" eine sehr effektive Methode zur Dechiffrierung der Vigènere–Verschlüsselung entwickelt hat.

[10)] Kultusministerium Sachsen–Anhalt: Rahmenrichtlinien Gymnasium Informatik, S. 37

Während sich symmetrische Chiffrierverfahren noch ohne mathematischen Einfluss darstellen lassen, tritt bei asymmetrischen Verfahren der mathematische Gehalt deutlich heraus. Neben der Einführung der Modulo–Rechnung sind hier zentrale Probleme der Zahlentheorie aufzuzeigen: Das RSA–Verfahren beruht auf dem Faktorisierungsproblem großer Primzahlprodukte. Dazu gehören im Unterricht Überlegungen zum Auffinden großer Primzahlen sowie zur Primfaktorzerlegung. Das ElGamal–Verfahren und der Diffi–Hellman Schlüsselaustausch basieren darauf, dass die diskrete Exponentialfunktion einfach zu berechnen ist, der diskrete Logarithmus allerdings sehr schwer. Die Beweise dieser Verfahren beruhen auf zentralen Sätzen der Zahlentheorie. Inwiefern diese Sätze im Unterricht behandelt werden können, wird in Kapitel "Unterrichtsbeispiele" dargelegt.

Informatik
Da sich die Kryptologie im hohem Maße informatischer Methoden bedient, lässt sich im Unterricht auch eine Verbindung zur Informatik aufzeigen. Abhängig von den Programmierkenntnissen der Schüler lassen sich insbesondere zu symmetrischen Verfahren Programme entwickeln; denn monoalphabetische Algorithmen sind leicht zu verstehen und schon bei geringen Programmiererfahrungen zu erstellen. Neben der Entwicklung eigener Programme können auch fertige Ver- und Entschlüsselungsprogramme im Unterricht eingesetzt werden.

Neben der Programmierung gehören auch die Einführung des Dualsystems und die Darstellung von Buchstaben durch den ASCII–Code bei der Behandlung moderner symmetrischer Chiffrierverfahren zu Lerninhalten des Unterrichtsfaches Informatik.

Im Bereich der asymmetrischen Chiffrierverfahren eignet sich der Einsatz eines Computeralgebra–Systems wie z. B. DERIVE. Neben der Berechnung von Potenzen lässt sich mit diesem auch der Zeitaufwand zur Faktorisierung großer Primzahlprodukte experimentell erfassen.

Geschichte
Aufgrund der geschichtlich gewachsenen Bedeutung und dem Einsatz kryptologischer Verfahren in vielen Kriegen, weist die Kryptologie auch eine Verbindung zum Unterrichtsfach Geschichte auf. Im Folgenden werden einige Beispiele hierfür dargestellt:

- Eines der bekanntesten historischen Beispiele der Steganographie betrifft die Schlacht zwischen dem Perserreich und Griechenland um 480 v. Chr. in der Bucht von Salamis bei Athen. Ein im persischen Exil lebender Grieche warnte die Spartaner vor dem persischen Angriff, indem er eine Nachricht über die persische Invasion auf eine hölzerne Schreibtafel ritzte und diese dann mit Wachs überzog. Auf diese Weise konnte er diese Tafel an den Wachen vorbei zum Spartanerkönig Leonidas schicken, der die Warnung erkannte und sich auf den persischen Angriff vorbereiten konnte[11)].
- Der römische Schriftsteller Gaius Suetonius Tranquillus (genannt Sueton), berichtet von einem kryptographischen Verfahren, das vom Feldherrn und Staatsmann C. Julius Caesar (100 - 44 v. Chr.) verwendet wurde – eine Verschiebechiffre, die auch heute noch "Caesar–Chiffre" genannt wird (vgl. Seite 5). Aufgrund der Einfachheit dieses Verfahrens bietet es sich zur Einführung in die Kryptologie an. Erwähnenswert dabei ist auch, dass diese Verschlüsselungsmethode noch 1915 von der russischen Armee verwendet wurde.

[11)] vgl. [14], S. 1051

- Ein sehr berühmtes Beispiel der Kryptographie betrifft auch die Geheimschrift der schottischen Königin Maria Stuart. Maria Stuart wurde 1586 wegen Verrates an der Königin Elisabeth I. zum Tode verurteilt. Der für die Sicherheit zuständige Minister Sir Francis Walsingham konnte ihre Beteiligung an einer Verschwörung gegen Elisabeth I. nachweisen, da man ihre Geheimschrift entziffern konnte[12)].
- Fortschritte in der Kryptanalyse gab es vor allem während des Ersten Weltkrieges, dessen Verlauf auch mit den Erfolgen der britischen Kryptanalytikern verbunden war. Der amerikanische Präsident Wilson zögerte in den Krieg einzutreten und versuchte diesen diplomatisch beizulegen. Im Januar 1917 verfasste der deutsche Außenminister Arthur Zimmermann ein Telegramm an den mexikanischen Präsidenten, in dem er ihm vorschlug, gemeinsam gegen Amerika in den Krieg zu ziehen, falls es sich nicht weiter neutral verhalten sollte. Das Telegramm wurde von den Briten abgefangen, entschlüsselt und an Amerika weitergeleitet, woraufhin die USA Deutschland den Krieg erklärte.
- In einer Unterrichtssequenz über die Enigma[13)] kann auf die Ereignisse des Zweiten Weltkrieges eingegangen werden. Auch in diesem Krieg waren die Alliierten in der Kryptanalyse erfolgreich, wodurch dessen Verlauf wesentlich beeinflusst wurde.

Wirtschaft und Recht
Sobald im Unterricht asymmetrische Chiffrierverfahren behandelt wurden, kann über rechtliche Aspekte der Kryptologie nachgedacht werden, wodurch eine fächerübergreifende Zusammenarbeit mit dem Fach Wirtschaft und Recht möglich ist.

Zu diesen Aspekten gehört z. B. die rechtliche Verankerung elektronischer Signaturen im “Gesetz über Rahmenbedingungen für elektronische Signaturen”, das seit 16. Mai 2001 in Kraft ist. Dieses kurzgenannte Signaturgesetz hat zum Ziel, eindeutige Rahmenbedingungen für elektronische Signaturen zu schaffen, um damit die Rechtssicherheit beim E–Commerce zu erhöhen. Durch die Behandlung des Signaturgesetzes lernen die Schüler einerseits, mit Gesetzestexten umzugehen. Andererseits erkennen sie, wie die Umsetzung theoretischen Wissens über elektronische Signaturverfahren in der Praxis durch Zertifizierungsstellen möglich ist.

In einer weiterführenden Diskussion kann die Rechtslage in Deutschland mit der in anderen Ländern verglichen werden. Viele Regierungen, wie z. B. die USA, Frankreich und China, sind gegen den Gebrauch kryptographischer Methoden. Der Grund hierfür ist, dass durch Verschlüsselung nicht nur Datenschutz gewährleistet werden kann, sondern dass sie auch von kriminellen Vereinigungen zur Geheimhaltung ihrer Taten genutzt wird. In den USA gehört Chiffrier–Software sogar zu den Rüstungsgütern und darf nicht ohne Genehmigung durch das Außenministerium exportiert werden[14)].

Deutsch
Kryptologie inspiriert auch Autoren, weshalb sich zahlreiche Beispiele von Geheimschriften in der Literatur wiederfinden. Durch Einsatz dieser Werke im Unterricht, schlägt Kryptologie auch eine Brücke zum Fach Deutsch.

---

12) vgl. [30], S. 15
13) Chiffriermaschine, die im Zweiten Weltkrieg vom deutschen Militär verwendet wurde.
14) vgl. [30], S. 365

Im Folgenden werden Geheimschriften aus der Literatur vorgestellt, die in einem Unterricht in Kryptologie fächerübergreifend eingesetzt werden könnten:

- Der Schriftsteller Joachim Ringelnatz hat in der "Bi–Sprache" ein Gedicht abgefasst. Bei dieser Verschlüsselung wird nach jedem Vokal ein "bi" eingefügt.
- Die Kinderbuchautorin Astrid Lindgren verwendet in "Kalle Blomquist lebt gefährlich" die Ror–Sprache. Hierzu wird nach jedem Konsonanten ein "o" eingefügt und danach der Konsonant wiederholt.
- Der amerikanische Schriftsteller Edgar Allan Poe stellt in "Der Goldkäfer" eine monoalphabetisch chiffrierte Nachricht aus Zahlen und Zeichen in den Mittelpunkt der Handlung und beschreibt auch das Vorgehen zu deren unbefugter Entschlüsselung.
- Die Abenteuer von Sherlock Holmes wurden vom britischen Schriftsteller Arthur Conan Doyles veröffentlicht. Dessen Geschichte "Die tanzenden Männchen" handelt von monoalphabetisch chiffrierten Nachrichten aus Strichmännchen–Zeichen. Auch hier wird das Vorgehen in der Kryptanalyse beschrieben.
- Im Roman "Reise zum Mittelpunkt der Erde" vom französischen Schriftsteller Jules Verne wird der Weg zum Erdinneren durch ein altes verschlüsseltes Dokument beschrieben, das es zu entziffern gilt.

3.4 Zusammenfassung

Nach der Beschreibung wichtiger kryptologischer Verfahren, werden in diesem Abschnitt Beispiele für den Einsatz der Kryptologie im Alltag dargelegt. Dadurch wird die große Bedeutung dieser Wissenschaft in der Praxis aufgezeigt. Dieser steht allerdings eine sehr geringe schulische Ausbildung in Kryptologie gegenüber. Es wird festgestellt, dass Sachsen–Anhalt die beste Möglichkeit für den Eingang der Kryptologie in die Schule bietet. Allerdings stellt diese Wissenschaft auch hier nur ein Wahlthema im Unterrichtsfach Informatik dar. Wie im nächsten Kapitel gezeigt wird, eignet sich dieses Wahlthema nur zur unterrichtlichen Behandlung symmetrischer Verschlüsselungsverfahren (siehe Seite 26).

Aufgrund der Allgegenwart kryptologischer Verfahren, ergibt sich damit ein Defizit in der schulischen Ausbildung. Erschwerend kommt hinzu, dass Kryptologie für fächerübergreifendes Unterrichten sehr geeignet erscheint. So umfasst Kryptologie Lerninhalte der Mathematik, der Informatik und des Faches Wirtschaft und Recht. Daneben erscheinen geschichtliche Ereignisse durch den Bezug zur Kryptologie aus einer neuen Perspektive. Außerdem wird die sonst schwierige Verbindung der Naturwissenschaften zum Fach Deutsch möglich.

4 Wissenschaftliches Umfeld

4.1 Kryptologie als Wissenschaft

Da es sehr viele Veröffentlichungen zur Kryptologie gibt, werden im Folgenden einige Publikationen vorgestellt, die als Hintergrundinformation zur Behandlung der Kryptologie im Unterricht geeignet sind und an den mathematisch interessierten Leser nur geringe Anforderungen stellen. Die Aufstellung erfolgt alphabetisch nach den Autoren.

- Von F. L. Bauer stammt mit "Entzifferte Geheimnisse – Methoden und Maximen der Kryptologie" ein Standardwerk über Kryptologie, das von historischen kryptologischen Verfahren bis zur modernen Kryptologie reicht und auch die Kryptanalyse ausführlich behandelt.

- A. Beutelspacher bietet in "Kryptologie – Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen" eine sehr gute Einführung in alle bekannten symmetrischen Chiffrierverfahren, die Techniken der Public–Key–Kryptologie sowie in Fragen zur Anonymität.

- An alle, "die sich über eine der faszinierendsten Entwicklungen der Mathematik und Informatik der letzten Jahre kundig machen wollen"[1] wendet sich A. Beutelspacher u. a. in "Moderne Verfahren der Kryptographie – Von RSA zu Zero–Knowledge". Wie bereits aus dem Titel ersichtlich, liegt der inhaltliche Schwerpunkt auf der Public–Key–Kryptographie, Zero–Knowledge–Protokollen[2] und auf der Anonymität bei Kommunikation mittels Computern.

- Großen Wert auf Primzahltests und die Primfaktorzerlegung in Zusammenhang mit asymmetrischen Chiffrierverfahren legt H. Horak in der dreiteiligen Artikelserie "Der bunte Zoo der Kryptologie" (vgl. [15]).

- Von R. Kippenhahn stammt mit "Verschlüsselte Botschaften – Geheimschrift, Enigma und Chipkarte" eine Einführung in bekannte Verfahren der Kryptologie, das die historischen Entwicklungen und deren Auswirkung auf die mit Kryptologie verbundenen Menschen sehr detailliert beschreibt und zahlreiche Beispiele überlieferter Geheimschriften enthält.

[1] [9], S. vii

[2] Durch Zero–Knowledge–Protokolle kann jemand seinen Kommunikationspartner von der Kenntnis eines Geheimnisses überzeugen, ohne dabei das geringste dieses Geheimnisses selbst zu verraten.

- Eine sehr ausführliche Behandlung sowohl der kryptographischen Verfahren als auch der Kryptanalyse liefert R. Wobst mit “Abenteuer Kryptologie. Methoden, Risiken und Nutzen der Datenverschlüsselung”. Dieses Werk widmet auch ein Kapitel den praktischen Anwendungen, wobei vor allem auf das Verschlüsselungsprogramm PGP eingegangen wird.

4.2 Didaktik der Kryptologie

4.2.1 Unterrichtssequenzen in Kryptologie

Im Folgenden werden Publikationen vorgestellt, die sich mit der unterrichtlichen Behandlung kryptologischer Inhalte befassen. Die Auflistung erfolgt nach steigender Komplexität und Vollständigkeit, mit der die Kryptologie vermittelt wird.

Jörn Zuber beschreibt in [37] Inhalte eines Wahlthemas Kryptologie für einen halbjährigen Grundkurs der 12. Jahrgangsstufe. Schwerpunkt dieses Unterrichts ist die Umsetzung von Chiffrierverfahren in der Programmiersprache JAVA–Script. Insofern werden vertiefte Kenntnisse in dieser Programmiersprache wie z. B. der Umgang mit Schleifen, Feldern und String–Funktionen vorausgesetzt. Die von Zuber dargelegten Lerninhalte beschränken sich auf symmetrische Chiffrierverfahren. Eingeführt wird in Kryptologie mit der monoalphabetischen Chiffrierung, wobei im einzelnen die

- Caesar–Chiffrierung
- multiplikative Substitution[3)]
- Transpositionschiffrierung
- Chiffrierung mit einem Schlüsselwort
- Verschlüsselung mit anderen Zeichen als Buchstaben

besprochen werden. Die Behandlung der polyalphabetischen Chiffrierung beschränkt sich auf die Vigenère–Verschlüsselung. Der Grundkurs endet mit einer Analyse der Schwächen von monoalphabetischen und polyalphabetischen Chiffrierungen.

Helmut Witten, Irmgard Letzner und Ralph–Hardo Schulz beschäftigen sich in der Artikelserie “RSA & Co. in der Schule” (vgl. [35]) mit der Frage, welche Inhalte der Kryptologie als Lerninhalte in der Schule geeignet sind. Dabei gehen sie davon aus, dass es “mit Sicherheit kein eigenes Fach Kryptologie geben”[4)] wird und die dargelegten Inhalte in anderen Fächern behandelt werden können. In der dreiteiligen Artikelserie werden zunächst Inhalte der Kryptologie erklärt

[3)] Monographische Substitution, bei der die Buchstaben des Alphabets mit den Zahlen von 1 bis 26 identifiziert werden. Die Verschlüsselungsfunktion V (mit dem Schlüssel s) lautet: $V(k) = (k \cdot s) \bmod 26$. Lediglich 12 multiplikative Chiffren erfüllen die Forderung nach der Eindeutigkeit einer Chiffrierung.

[4)] [35], v. 18, Heft 3/4, S. 59

und anschließend Hinweise zu deren Behandlung im Mathematikunterricht und im Informatikunterricht gegeben. Der erste Teil beginnt mit der Analyse natürlicher Sprachen. Darauf aufbauend wird empfohlen, monoalphabetische Chiffrate von Schülern entziffern zu lassen. Nach den Autoren sollte hierzu im Mathematikunterricht auf fertige Programme zurückgegriffen werden. Im zweiten Teil werden die Caesar–Verschlüsselung und deren Verallgemeinerung durch die Chiffrierung mit einem Schlüsselwort sowie die Vigenère–Verschlüsselung vorgestellt. Daran schließt sich die Kryptanalyse an, wobei sowohl der Kasiski- als auch der Friedman–Test dargelegt werden. Für den Mathematikunterricht wird empfohlen, mit der Caesar–Chiffrierung zu beginnen und zur Ver- und Entschlüsselung eine Chiffrierscheibe[5)] zu verwenden. Im Informatikunterricht bietet es sich nach den Autoren an, Programme zur Ver- und Entschlüsselung zu erstellen, wobei umfangreiche Programmierkenntnisse vorausgesetzt werden. Der letzte Teil der Veröffentlichung handelt von Flusschiffren und einem geschichtlichen Rückblick auf die Verwendung von Vernams one–time–pad. Für den Mathematikunterricht werden Anregungen gegeben, wie die Modulo–Rechnung eingeführt werden kann und das Basteln eines einfachen Rotorgeräts empfohlen. Im Informatikunterricht sollte die Verschlüsselung nach Vernam programmiert werden und das Erzeugen von Zufallszahlen diskutiert werden.

Während der Teilnahme am ersten Pilotversuch zur Durchführung eines Kompaktstudiums "Informatik als Zusatzfach" an der Technischen Universität München von 1995 bis 1997, entstanden "Bausteine zur Didaktik der Informatik, in die die Erkenntnisse der Studierenden direkt einfließen konnten."[6)] Im Baustein "Kryptologie" (vgl. [13]) stellen Helmut Günthner und Josef Schmailzl eine Unterrichtssequenz für einen Wahlunterricht Informatik vor, in dem Programme zu kryptologischen Verfahren entwickelt werden. Sämtliche Programme werden in der Programmiersprache Gofer erstellt. Die vorgestellte Unterrichtssequenz beginnt mit der Behandlung symmetrischer Chiffrierverfahren. Dabei werden Algorithmen, Funktionen und Aufgaben zur

- Caesar–Chiffrierung
- Monoalphabetischen Substitution
- Vigenère–Verschlüsselung

vorgestellt. Zielgruppe dieses Unterrichts sind Schüler des Gymnasiums ab der 8. Jahrgangsstufe. Im "Rahmen eines Pluskurses für besonders begabte Schüler in der Oberstufe"[7)] wird im zweiten Teil der Veröffentlichung das RSA–Verfahren als Beispiel eines asymmetrischen Chiffrierverfahrens vorgestellt. Besonderer Wert wird hier auf die Bedienung von ARIBAS gelegt, einem "Interpreter, der für das ganzzahlige Rechnen mit großen Zahlen und das genaue Rechnen mit Gleitkomma–Zahlen sehr gut geeignet ist."[8)]

Ausgehend von der Computervernetzung in Schulen legt Rüdeger Baumann in [3] dar, welchen Beitrag der Informatikunterricht zur Informationssicherheit leisten kann. Insofern werden

[5)] Eine Chiffrierscheibe besteht aus zwei kreisförmigen Scheiben unterschiedlicher Größe, an deren Kreisrändern das Alphabet aufgeschrieben ist. Auf diese Weise kann bei einer Verschiebechiffre das Geheimtextalphabet durch entsprechende Anordnung der kleineren Scheibe in der größeren abgelesen werden.

[6)] [13], S. 3

[7)] [13], S. 8

[8)] [13], S. 22

kryptologische Verfahren und Algorithmen im Hinblick auf die Gewährleistung von Sicherheit im Datennetz behandelt. Nach Baumann ist im Anfangsunterricht Informatik zunächst ein Kurs zum systematischen Programmieren zu durchlaufen. Erst danach werden kryptologische Verfahren im Unterricht besprochen. Im Bereich der symmetrischen Chiffrierverfahren wird auf die monoalphabetische Substitution einschließlich deren Umsetzung in einem Programm eingegangen. Als Beispiel für asymmetrische Verschlüsselungen wird das Chiffrierverfahren nach ElGamal behandelt, da die erforderlichen mathematischen Vorkenntnisse geringer sind als beim RSA–Verfahren. Um die Sicherheit dieses Verfahrens zu diskutieren, wird der Begriff der "Einwegfunktion" eingeführt und am Beispiel der diskreten Exponentialfunktion erläutert. Da Informationssicherheit auch Schutz der Daten vor Veränderungen unbefugter Personen bedeutet, sollten nach Baumann anschließend die

- Authentisierung mittels Kennwort
- Authentisierung nach dem Frage–Antwort–Verfahren auf Basis von Zufallszahlen
- Schlüsselvereinbarung nach Diffie–Hellmann

im Unterricht behandelt werden.

Klaus–Cl. Becker und Albrecht Beutelspacher beschäftigen sich in [5] mit der Datenverschlüsselung, einer Anwendung der Kryptologie. Bevor ein Überblick über Verschlüsselungsverfahren gegeben wird, wird die zunehmende Bedeutung der Kryptologie beschrieben und an Beispielen veranschaulicht. Anschließend legen die Autoren das Verschlüsselungsverfahren IDEA (International Data Encryption Algorithm) genau dar und beschreiben die Schlüsselvereinbarung nach Diffie und Hellman in groben Zügen. Dabei legen sie Wert auf schnelles Potenzieren mit dem "Square and Multiply"–Algorithmus, der in Pseudocode angegeben wird. Der RSA–Algorithmus wird als Beispiel dafür genannt, wie Zahlentheorie zur Lösung praktischer Aufgaben beitragen kann. An ein vorgerechnetes Beispiel für die RSA–Verschlüsselung schließen sich Überlegungen zur Sicherheit von Verschlüsselungsverfahren an.

4.2.2 Unterrichtliche Behandlung bestimmter Aspekte der Kryptologie

Aufgrund der Zunahme elektronischer Vertragsabschlüsse, beschäftigt sich Rüdeger Baumann in [4] mit der unterrichtlichen Behandlung des Themas "Sicherheit im elektronischen Rechtsverkehr". Dazu werden im ersten Teil des Artikels die aktuelle Rechtslage elektronischer Dokumente sowie die Anforderungen an digitale Unterschriften aufgezeigt. Anschließend wird die digitale Signatur mittels des RSA–Verfahrens beschrieben und mit einem DERIVE–Protokoll vorgeführt. Im zweiten Teil werden Hashfunktionen und darauf aufbauende Signiersysteme beschrieben. Daran schließen sich Überlegungen zur Sicherheit der digitalen Unterschrift an. Der Artikel endet, indem Probleme der digitalen Unterschrift sowie deren Lösung in der Praxis aufgezeigt werden.

Martin Epkenhans stellt in [11] den mathematischen Gehalt der Kryptologie dar und rechtfertigt auf diese Weise die Kryptologie als Unterrichtsgegenstand im Leistungskurs Mathematik

und damit als Themengebiet für Facharbeiten. Im Artikel wird zunächst ein Überblick über kryptologische Verfahren unter Betonung des mathematischen Gehalts gegeben. Anschließend beschreibt Epkenhans die Einbettung der Kryptologie in den Mathematikunterricht. Hierfür werden Hinweise zu Unterrichtszielen, zur Einführung der Kryptologie sowie zu Lernvoraussetzungen gegeben und Möglichkeiten des Computereinsatzes aufgezeigt. Zur Begründung des Unterrichtsgegenstands Kryptologie führt Epkenhans die Motivation der Schüler, die Notwendigkeit hoher Sicherheitsstandards sowie fächerübergreifende Aspekte auf. Durch die Behandlung der Kryptologie im Leistungskurs Mathematik, entstehen Fragen, auf die im Unterricht nicht ausreichend eingegangen werden kann. Auf diese Weise entstehen Themen für Facharbeiten. Im letzten Teil des Artikels [11] werden deshalb Vorschläge für Facharbeitsthemen aufgeführt.

In Anlehnung an einen Lehrerfortbildungskurs beschreibt Ralph–Hardo Schulz in [29] die Vermittlung einfacher experimenteller Erfahrungen zur Primfaktorzerlegung. Da die Sicherheit der RSA–Verschlüsselung auf der Falltüreigenschaft der Produktbildung zweier Primzahlen gründet, stellt dies ein Thema der Kryptologie dar. Nach einem Überblick über die Rolle der Primzahlen und deren Bedeutung für den RSA–Algorithmus, wird der Zeitaufwand für die Faktorisierung großer Zahlen experimentell erfasst. Dazu werden mit einem DERIVE Programm Zahlen in ihre Primfaktoren zerlegt, wobei die benötigte Rechenzeit und die Stellenzahl der Zahlen erfasst werden. Die anschließende graphische Darstellung zeigt, dass die Rechenzeit in Abhängigkeit von der Stellenanzahl der Zahlen exponentiell ansteigt.

Peter Batzer stellt in [1] Grundlagen zu einer Unterrichtssequenz über die Enigma – der deutschen Chiffriermaschine im Zweiten Weltkrieg – vor. Dazu werden zunächst in einem geschichtlichen Abriss die Entwicklung und die Bedeutung der Enigma vorgestellt sowie Fehler in deren Handhabung mit den entsprechenden Folgen beschrieben. Das Gewicht der Unterrichtssequenz liegt auf der Analyse der Funktionsweise der Enigma. Deshalb werden schrittweise hierfür benötigte mathematische Kenntnisse vermittelt. Dazu gehören

- Permutationen der Ziffern 0 bis 9,
- das Verfahren, wie die Enigma neue Permutationen erzeugt und
- die Verkettung von Permutationen bei der Enigma.

Anschließend folgt die Bedienungsanleitung eines vom Autor entwickelten Simulationsprogramms “Ziffernenigma” und die Vorstellung von Einsatzmöglichkeiten für dieses Programm im Unterricht. Dabei wird besonderer Wert auf die Bedeutung des Reflektors gelegt, sowie auf den Nachweis, dass die Enigma eigene Geheimtexte dechiffrieren kann.

4.2.3 Veröffentlichte Arbeitshefte zur Kryptologie

In der Zeitschrift “mathematik lehren” ist 1995 von Albrecht Beutelspacher das Schülerarbeitsheft “Mathe–Welt–Geheimschriften” erschienen[9)]. Der Einstieg in Kryptologie erfolgt in diesem durch Beispiele von einfachen Geheimschriften, wie z. B. der Geheimschrift aus “Kalle

[9)] vgl. [7]

Blomquist lebt gefährlich" von Astrid Lindgren. Anschließend wird die Caesar–Verschlüsselung erklärt und diese Methode auf ihre Schwachstellen untersucht. Als Beispiel einer polyalphabetischen Chiffrierung wird die Vigenère–Verschlüsselung erläutert, sowie deren Entschlüsselung anhand von Beispielen in zwei Teilen dargelegt. Im ersten Teil geht man davon aus, dass die Schlüsselwortlänge bekannt ist. Im zweiten Teil wird untersucht, wie man die Länge des Schlüsselwortes mit Hilfe des Kasiski–Tests erkennen kann. Anschließend erfolgt ein Ausblick, wie perfekte Sicherheit erreicht werden kann.

Ebenfalls in der Zeitschrift "mathematik lehren" wurde der Schüler–Lesetext "Von Cäsar zum Internet" von Julia Berlin und Nicole Roth–Sonnen (vgl. [6]) veröffentlicht. In diesem Lesetext beschäftigen sich die Schüler Max und Lisa mit der Caesar–Chiffre und der Vigenère–Verschlüsselung. Als Beispiel einer asymmetrischen Verschlüsselung wird unter Einführung der Modulo–Rechnung das RSA–Verfahren herangezogen.

4.3 Zusammenfassung

In diesem Kapitel wird zunächst eine Auswahl leicht verständlicher Literatur über Kryptologie vorgestellt. Diese enthält neben wissenschaftlichen Abhandlungen über Kryptologie auch Werke, die besonderen Wert auf Beispiele, historische Auswirkungen oder den Gegenwartsbezug von Verschlüsselungsverfahren legen. Auf diese Weise soll dem interessierten Leser die Literaturauswahl erleichtert werden.

Neben diesen Werken über die Wissenschaft "Kryptologie" existieren auch Veröffentlichungen, die sich mit der unterrichtlichen Behandlung kryptologischer Inhalte befassen. Von diesen werden zunächst solche Publikationen zusammengefasst, die in Kryptologie einen Lerninhalt für den Informatik- oder Mathematikunterricht sehen. Hierauf folgt die Darstellung von Artikeln, die sich auf bestimmte Teilgebiete der Kryptologie beschränken und deren Eignung für den Schulunterricht untersuchen. Die eher praktisch orientierte Zeitschrift "mathematik lehren" publizierte schließlich noch Arbeitsblätter zur Kryptologie, die kurz beschrieben werden.

5 Kryptologie als Wahlfach

5.1 Berechtigung eines Unterrichts in Kryptologie

Im Kapitel “Kryptologie im Alltag” wurde anhand von Beispielen die hohe gegenwärtige Bedeutung kryptologischer Verfahren aufgeführt. Daneben wurde gezeigt, dass kryptologische Inhalte in den aktuellen Lehrplänen der Schulen in der Bundesrepublik Deutschland nicht enthalten sind bzw. nur ansatzweise behandelt werden können. Lediglich im Bundesland Sachsen–Anhalt wird in der gymnasialen Oberstufe Kryptologie als Wahlthema im Informatikunterricht ermöglicht. Nachteilig wirkt sich hier allerdings die Schwerpunktsetzung auf die Umsetzung kryptologischer Verfahren in einer Programmiersprache aus (siehe Seite 26). Dadurch werden wichtige kryptologische Inhalte wie z. B. die asymmetrischen Chiffrierverfahren von der unterrichtlichen Behandlung ausgeschlossen. Auch bisherige Veröffentlichungen über die Behandlung von Kryptologie im Unterricht sehen vor, Aspekte der Kryptologie im Mathematik- oder Informatikunterricht einfließen zu lassen. Eine umfassende kryptologische Ausbildung kann dadurch nicht erreicht werden.

Ein Unterricht in Kryptologie bietet nicht nur eine fundierte Ausbildung in dieser bedeutenden Wissenschaft. Wie bereits erläutert, ermöglicht dieser auch vielfältiges fächerübergreifendes Unterrichten. Außerdem sind nach Günthner und Schmailzl “Schüler der Unter- und Mittelstufe [...] am Thema Geheimschriften im Allgemeinen sehr interessiert. Sie bringen von sich aus eine Vorliebe für das Geheime mit und sind bestrebt, geheime Botschaften zu entschlüsseln”[1)].

Die dargelegte mangelnde Ausbildung in Kryptologie sowie positive fächerübergreifende Möglichkeiten und das Interesse von Schülern, befürworten einen Unterricht in Kryptologie, können aber die Einführung eines Unterrichts in dieser Wissenschaft nicht rechtfertigen. Deshalb soll in diesem Kapitel ein Unterricht in Kryptologie im Rahmen des Wahlfachangebots an allgemein bildenden Schulen berechtigt werden.

Diese Berechtigung erfährt der Kryptologieunterricht, sofern er einen Beitrag zur Bildungs- und Erziehungsarbeit der Schulen leistet. Hierzu werden zunächst die gesetzlichen Aufgaben allgemein bildender Schulen erläutert, wobei die gesetzlichen Vorschriften des Bundeslandes Bayern herangezogen werden. Daran anknüpfend, werden schließlich die Beiträge von Kryptologie zur Allgemeinbildung, zur Berufsvorbereitung und zur Vorbereitung auf ein Hochschulstudium dargelegt.

[1)] [13], S. 6

5.1.1 Aufgaben allgemein bildender Schulen

Die Bildungs- und Erziehungsarbeit allgemein bildender Schulen wird durch das Bayerische Erziehungs- und Unterrichtsgesetz (BayEUG) festgelegt. Nach Art. 6 BayEUG sind allgemein bildende Schulen

1. die Grundschule,
2. die Hauptschule,
3. die Realschule,
4. das Gymnasium,
5. die Schulen des Zweiten Bildungsweges.

Die Grundschulen werden in den folgenden Ausführungen nicht betrachtet, da diese auf die weiterführenden Schulen (d. h. Hauptschule, Realschule und Gymnasium) vorbereiten und damit keinen Abschluss im engeren Sinn vermitteln. Hinzu kommt, dass die Schüler der Grundschule nicht über die erforderliche Abstraktionsfähigkeit und die notwendigen mathematischen Kenntnisse für einen erfolgreichen Unterricht in Kryptologie verfügen. Sofern die Schulen des Zweiten Bildungsweges zum Realschulabschluss bzw. zur allgemeinen Hochschulreife führen, finden die Erläuterungen zu Realschulen bzw. zu Gymnasien entsprechend Anwendung.

Nach Art. 7ff des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen vermittelt

- die Hauptschule “eine grundlegende Allgemeinbildung, bietet Hilfen zur Berufsfindung und schafft Voraussetzungen für eine qualifizierte berufliche Bildung”.
- die Realschule “eine breite allgemeine und berufsvorbereitende Bildung”.
- das Gymnasium “die vertiefte allgemeine Bildung, die für ein Hochschulstudium vorausgesetzt wird”.

Folglich werden die gesetzlichen Aufgaben von allgemeinbildenden Schulen durch

- Allgemeinbildung,
- Berufsvorbereitung und durch
- Studienvorbereitung

bestimmt[2)].

Zusammenfassend gilt damit: Sofern gezeigt werden kann, dass eine kryptologische Ausbildung zur Allgemeinbildung, Berufsvorbereitung und zur Studienvorbereitung beisteuert, trägt ein Unterricht in Kryptologie dazu bei, die gesetzlichen Aufgaben allgemein bildender Schulen zu erfüllen. Damit erhält dieser Unterricht seine Berechtigung.

In den folgenden Abschnitten wird deshalb erläutert, inwiefern ein Unterricht in Kryptologie zur Allgemeinbildung, Berufsvorbereitung und zur Studienvorbereitung beträgt.

[2)] vgl. auch [17]

5.1.2 Beitrag von Kryptologie zur Allgemeinbildung

Mit Allgemeinbildung verband ursprünglich der als Begründer der Didaktik geltende Pädagoge Johann Amos Comenius (1592 - 1670) das Ziel, allen Menschen alles zu lehren. Auch im Zeitalter der Aufklärung während des 17. und 18. Jahrhunderts ist Allgemeinbildung durch das Bestreben geprägt, alles Wissen zu sammeln und der Bevölkerung zugänglich zu machen. Im 19. Jahrhundert beabsichtigten Neuhumanisten wie Wilhelm von Humboldt (1767 - 1835) in Schulen die für die Emanzipation des Menschen benötigte Allgemeinbildung einzuführen. Seit dieser Zeit ist Allgemeinbildung bedeutungsgleich zu Bildungskanon.

Zur Bestimmung des Begriffs "Allgemeinbildung" wird in dieser Arbeit auf die Definition nach Wolfgang Klafki zurückgegriffen. Klafki gilt als einer der bedeutendsten Erziehungswissenschaftler der letzten 50 Jahre, ist Mitbegründer der Bildungstheoretischen Didaktik und hat diese zur Kritisch–Konstruktiven Didaktik weiter entwickelt.

Anknüpfend an Comenius und an die Ziele der Aufklärung ist nach Klafki Allgemeinbildung in dreifachem Sinn zu bestimmen:

- Allgemeinbildung muss Bildung für alle sein.
- Allgemeinbildung muss allseitige Bildung sein.
- Allgemeinbildung muss eine Bildung durch das Allgemeine sein.[3)]

Dabei muss sich das Allgemeine "vor allem an aktuell–historischer Sicht als allgemein erweisen, muss nach Klafki 'Schlüsselproblem' der Gegenwart der betroffenen Schüler sein und sie über sich in die Gegenwart oder zumindest einen äußerst weiten Bereich dieser Gegenwart hineinführen"[4)].

Zusammenfassend gilt somit, dass Allgemeinbildung nach Klafki "eine Bildung für alle Schüler der jeweiligen Lerngruppe, deren allseitige und nicht bloß einseitige Bildung sowie deren Bildung durch bzw. an allgemeinen Themen"[5)] ist.

5.1.2.1 Bildung für alle

Nach Klafki beansprucht Allgemeinbildung zunächst Bildung für alle zu sein. Diese Forderung zielt auf Chancengleichheit aller Kinder, unabhängig von deren gesellschaftlicher Herkunft.

Aufgrund der Allgegenwart kryptologischer Einflüsse und Notwendigkeiten ist eine entsprechende Ausbildung grundsätzlich für Schüler aller Bevölkerungsschichten interessant. Außerdem beschränken sich notwendige Vorkenntnisse zum Besuch eines Wahlfaches Kryptologie auf grundlegende mathematische Fähigkeiten, so dass Krytologie als Unterrichtsfach an allen allgemeinbildenden Schulen – d. h. an Hauptschulen, Realschulen und Gymnasien – angeboten werden kann.

[3)] vgl. [22], S. 52ff
[4)] [26], S. 76/77
[5)] [26], S. 78

Wird folglich Kryptologie als Wahlfach für bestimmte Jahrgangsstufen angeboten, erhalten damit alle angesprochenen Schüler die Möglichkeit zur Bildung, da ein Unterricht in Kryptologie unabhängig von sozialer Herkunft und belegten Wahlpflichtfächergruppen besucht werden kann. Insofern stellt ein Kryptologieunterricht Bildung für alle Schüler einer Schule dar.

5.1.2.2 Allseitige Bildung

Die Forderung Klafkis nach allseitiger Bildung zielt auf eine vielseitige Entwicklung von Interessen und Kompetenzen. Darunter versteht man ein Lernen, das

- sowohl kognitive, als auch soziale und emotionale Lernziele umfasst und diese nicht nur ergebnisorientiert, sondern auch prozessorientiert anstrebt.
- nicht auf den klassischen Bildungskanon beschränkt ist, sondern auch moderne Themen im Interesse von Schülern einschließt.

Bezüglich der Forderung nach kognitiven, sozialen und emotionalen Lernzielen, sollen zunächst die Lernziele aufgeführt werden, die H. Günthner und J. Schmailzl in [13] in Kryptologie als Lerninhalt im Informatikunterricht anstreben:

1. Einführung in die Kryptographie und Kyptanalyse (Wissen).
2. Freude beim Verschlüsseln und Entschlüsseln von Texten (emotioneller Bereich).
3. Einblick in Sicherheitsaspekte der heutigen Informationsgesellschaft (Auseinandersetzung mit gesellschaftlichen Problemen).
4. Notwendigkeit des Datenschutzes (Wertorientierung).
5. Einsatz des Computers als beschleunigendes Werkzeug zeitaufwendiger Tätigkeiten (Können und Anwenden).
6. Festigung des Umgangs mit Listen und Rekursionen (Können und Anwenden).

Diese Lernziele zeigen, dass mit Kryptologie auch ohne Einbeziehung der Programmierung (Lernziele 5 und 6) sowohl kognitive als auch affektive Lernziele erreicht werden können. Daneben kann in einem Unterricht in Kryptologie auch ein Beitrag zur Wertorientierung geleistet werden. Soziale Lernziele werden durch Diskussionen über die Notwendigkeit des Datenschutzes erreicht. Durch kritische Analysen von Chiffriermethoden im Rahmen der Kryptanalyse werden außerdem die Kritik- und die Urteilsfähigkeit gefördert und die Schüler somit zur Mündigkeit erzogen.

Wird die Programmierung mit einbezogen, werden kognitive Lerninhalte in Kryptologie und Programmierkenntnisse auf unterschiedlichen Intensitätsstufen erreicht und die Fähigkeit zur Abstraktion gefördert. Die Informationsmedien werden als Werkzeug des Verschlüsselns als auch des unbefugten Dechiffrierens von Kryptogrammen erlebbar. Auf diese Weise entwickeln Schüler einen verantwortungsbewussten und kritischen Umgang mit Informationstechnologien.

Die zweite Forderung Klafkis, auch moderne Themengebiete im Interesse von Schülern in den Schulunterricht aufzunehmen, beansprucht geradezu die Vermittlung kryptologischer Inhalte. Zum einen ist Kryptologie im heutigen Informationszeitalter bedeutsamer denn je. Durch die hohe praktische Bedeutung kann dadurch das Interesse der Schüler angesprochen werden. Zum anderen stellt Kryptologie für Schüler von sich aus ein sehr interessantes und ansprechendes Themengebiet dar. Kinder und Jugendliche weisen im allgemeinen eine hohe Neugierde im Hinblick auf Geheimschriften und deren Entzifferung auf.

Zusammenfassend gilt, dass durch einen Kryptologieunterricht eine vielseitige Bildung in kognitiven, affektiven und sozialen Bereichen erreicht, ein Beitrag zum Aufbau eigener Wertvorstellungen geleistet und ein für Schüler interessantes modernes Thema in den Schulunterricht integriert wird.

5.1.2.3 Bildung durch das Allgemeine

Nach Klafki bedeutet Bildung im Medium des Allgemeinen "ein geschichtlich vermitteltes Bewußtsein von zentralen Problemen der Gegenwart und – soweit voraussehbar – der Zukunft zu gewinnen"[6]. Dadurch entwickelt sich nach Klafki "Einsicht in die Mitverantwortlichkeit aller angesichts solcher Probleme und Bereitschaft, an ihrer Bewältigung mitzuwirken"[7].

Im Folgenden wird deshalb dargelegt, dass Kryptologie einerseits ein zentrales Problem der Gegenwart und der Zukunft darstellt. Andererseits aber auch aus Problemen in der Vergangenheit entstand und somit eine geschichtliche Entwicklung aufweist.

Kryptologie als zentrales Problem der Gegenwart und der Zukunft
Angesichts der drastischen Ausweitung des Internets und des elektronischen Datenverkehrs sieht sich unsere gegenwärtige Gesellschaft mit vielseitigen Sicherheitsproblemen konfrontiert. Dazu gehören z. B.

- Wie kann eine vertrauliche Kommunikation erreicht werden?
- Wie kann die Speicherung von personenbezogenen oder geheimen Daten gesichert werden?
- Wie kann der Empfänger einer Nachricht sicher sein, dass diese vom angegebenen Absender stammt und von Dritten nicht verändert wurde?
- Wie kann ein Chipkartenterminal die Identität des Kommunikationspartners überprüfen?
- Wie kann bei der Abwicklung von rechnernetzgestützten Alltagsgeschäften Datenschutz und Verbindlichkeit erreicht werden?[8]

Diese Fragen zeigen die Notwendigkeit kryptologischer Verfahren in heutiger Zeit auf. Deshalb forderten bereits 1997 H. Günthner und J. Schmailzl in [13], dass im Informatikunterricht

[6] [22], S. 56
[7] [22], S. 56
[8] vgl. [16]

in höheren Jahrgangsstufen Kryptologie behandelt werden sollte und dabei folgende Aspekte angesprochen werden sollten:

1. ”Daten, die gespeichert sind oder übertragen werden, dürfen von Unbefugten nicht gelesen oder verändert werden.
2. Bei elektronischen Geldüberweisungen muss geprüft werden können, ob der Auftrag von einem hierfür Berechtigten gegeben worden ist.
3. Elektronische Briefe sollten auch vertraulich gesendet und unterschrieben werden können.”[9)]

Diese Forderungen bedingen die unterrichtliche Vermittlung symmetrischer und asymmetrischer Chiffrierverfahren. Verstärkt wird die Bedeutung der Kryptologie dadurch, dass der elektronische Datenverkehr und damit der Wunsch nach Sicherheit in den letzten Jahren zugenommen hat.

Kryptologie als geschichtlich gewachsenes Problem
Obwohl Kryptologie eine zentrale Bedeutung in der gegenwärtigen Zeit darstellt, weist diese Wissenschaft auch eine jahrtausende alte Vergangenheit auf. Erste Berichte über den Gebrauch der Steganographie, einer zur Kryptographie verwandten Wissenschaft über das Verbergen geheimer Nachrichten, finden sich im Werk “Historien” des griechischen Historikers Herodot (ca. 484 bis 425 v. Chr.).

Da die symmetrischen Chiffrierverfahren hauptsächlich in zwei Verfahren – die Transposition und die Substitution – zerfallen, sind Entwicklungen beider Verschlüsselungstechniken in der Geschichte zu beobachten. Eine der ersten Chiffren durch Transposition erfolgte mit der Skytale, die die Spartaner im 5. Jahrhundert verwendeten. “Eine der frühesten Beschreibungen der Verschlüsselung durch Substitution erschien im Kāmasūtra, einem Text, den der brahmanische Gelehrte Wātsjājana im 4. Jahrhundert n. Chr. schrieb, allerdings unter Rückgriff auf Handschriften, die auf das 4. Jahrhundert v. Chr. zurückgingen.”[10)]

Zur Erfindung der Kryptanalyse musste die Entwicklung in der Mathematik, der Statistik und in der Sprachwissenschaft erst weiter vorankommen. So waren es die Araber, die die Kryptanalyse mithilfe der Buchstabenhäufigkeit erkannten. Die “früheste bekannte Beschreibung dieser Technik stammt von einem Gelehrten des neunten Jahrhunderts.”[11)]

In Europa fand die Kryptographie erst im 14. Jahrhundert Anwendung. Doch angesichts der Leistungen der Kryptanalysten, der Erfindung des Telegraphen und des Funkverkehrs kam es hier zur Entwicklung immer besserer Verschlüsselungsverfahren. Schließlich wurde die Forschung in Kryptologie auch zu Zeiten der beiden Weltkriege vorangetrieben, da hier das Bedürfnis nach sicherer Kommunikation und das Bestreben, abgefangene Geheimtexte zu entschlüsseln, besonders hoch war.

Nachteile bisheriger Chiffrierverfahren veranlassen Wissenschaftler bis heute die Forschung in Kryptologie weiter zu treiben. Im Jahr 1978 gelang dadurch die Entwicklung asymmetrischer

[9)] [13], S. 6
[10)] [30], S. 24
[11)] [30], S. 33

Chiffrierverfahren, die völlig neue Möglichkeiten der Verschlüsselung und Authentikation ermöglichen.

Zusammenfassend lässt sich festhalten, dass Kryptologie nicht nur ein zentrales Problem der Gegenwart sowie der Zukunft darstellt, sondern auch eine lange historische Entwicklung aufweisen kann. Der Forderung nach der Allgemeinheit dieses Unterrichtsgegenstandes ist damit genüge getan.

5.1.3 Beitrag von Kryptologie zur Berufsvorbereitung

Kryptologie dient im Rahmen der Berufsvorbereitung vor allem dazu, einen kritischen Umgang mit Informations- und Kommunikationsmedien zu entwickeln und Kenntnisse zur Gewährleistung von Datensicherheit zu vermitteln. Fähigkeiten in diesen Bereichen sind nicht nur in den informationstechnologischen Berufen von Interesse. So können z. B.

- Unternehmen durch Verschlüsselung vertrauliche Nachrichten, die per E-Mail verschickt werden, schützen.
- Betriebsgeheimnisse durch kryptographische Hashfunktionen unauslesbar abgespeichert werden.
- Händler und Banken mittels Verschlüsselungen finanzielle Transaktionen schützen.
- Behörden bei der Speicherung personenbezogener Daten durch Zugriffsberechtigungen die Privatssphäre der betroffenen Personen schützen.

Dies ist angesichts der zunehmenden Bedeutung des Internets und des elektronischen Datenverkehrs von großem Interesse. Nicht nur dass E-Mails leicht abgefangen, gelesen oder verändert werden können. Auch haben Systemadministratoren Zugang zu Passwortdateien, so dass Passwörter entsprechend unauslesbar abgespeichert werden müssen.

Das Sicherheitsbedürfnis in der Berufs- und Arbeitswelt zeigt sich auch nach der Globus Infografik GmbH. Danach wurden im Jahr 2004 bei 31% der Unternehmen in Deutschland mit Internetanschluss Daten zur Übertragung verschlüsselt. In 44% aller Unternehmen wurden PIN–Codes eingesetzt und 10% bedienten sich der digitalen Unterschrift als Sicherungsmechanismus.

5.1.4 Beitrag von Kryptologie zur Studienvorbereitung

Für Gymnasiasten ist es von Bedeutung, dass ein Wahlunterricht in Kryptologie auch einen Beitrag zur Studienvorbereitung leistet. Dies ist vor allem in naturwissenschaftlichen Studiengängen der Fall. Denn Vorlesungen in Kryptologie werden insbesondere in den Studiengängen Informatik, Elektrotechnik und Mathematik angeboten.

Angesichts der zunehmenden Bedeutung der Kryptologie setzen auch andere Studienrichtungen Kenntnisse in Kryptologie voraus. Dies betrifft z. B. juristische Studien, die sich mit Rechtsfragen kryptologischer Verfahren und der elektronischen Unterschrift auseinandersetzen.

Neben direkten Lehrangeboten in Kryptologie wird die Studienvorbereitung der Schüler durch ein Unterrichtsfach Kryptologie auch dadurch gefördert, dass Verschlüsselungsverfahren vorgestellt, kritisch überprüft, durch Kryptanalyse gebrochen und durch neue Verfahren ersetzt werden. Dadurch wird den Schülern vor Augen geführt, dass wissenschaftliche Erkenntnisse einem ständigen Wandel unterliegen und die Bereitschaft zur Weiterbildung gestärkt.

Schließlich kann Kryptologie auch die Bereitschaft zur Aufnahme eines mathematischen Studienganges fördern, denn in asymmetrischen Verschlüsselungsverfahren zeigt sich, wie die Zahlentheorie zur Lösung praktischer, gesellschaftlicher Probleme beitragen kann.

5.1.5 Zusammenfassung

Wenn ein neues Unterrichtsfach an allgemeinbildenden Schulen eingeführt werden soll, ist zu prüfen, ob der betreffende Lerngegenstand einen Beitrag zur Bildungs- und Erziehungsarbeit der Schulen leistet. Hierfür wird in diesem Kapitel erläutert, dass ein Unterrichtsfach zum Bildungs- und Erziehungsauftrag beiträgt, wenn es zur Allgemeinbildung, Berufsvorbereitung und Studienvorbereitung einen Beitrag leistet.

Anschließend wird der sehr umfassende Begriff “Allgemeinbildung” konkretisiert und gemäß Klafki durch die drei Ebenen “Bildung für alle”, “Allseitige Bildung” und “Bildung durch das Allgemeine” bestimmt. Im Anschluss daran wird erläutert, dass Kryptologie als Unterrichtsfach den drei Kriterien von Allgemeinbildung genügt und zur Vorbereitung junger Menschen auf den Beruf bzw. auf ein Hochschulstudium beiträgt.

Folglich werden durch ein Wahlfach “Kryptologie” die Forderungen des Bildungs- und Erziehungsauftrags der allgemeinbildenden Schulen erfüllt, wodurch dieser Unterricht seine Berechtigung erfährt.

5.2 Didaktischer Ort eines Unterrichts in Kryptologie

Nachdem im vorhergehenden Kapitel ein Unterricht in Kryptologie an allgemeinbildenden Schulen Eingang fand, folgen nun Überlegungen zum didaktischen Ort dieses Unterrichts. Zu berücksichtigen ist hierbei, dass sich Kryptologie als Wissenschaft in hohem Maße mathematischer und rechnergestützter Methoden bedient. “Mathematische Disziplinen, die nach dem heutigen Stand für die Kryptologie von Belang sind, umfassen unter anderem: Zahlentheorie, Gruppentheorie, Kombinatorik, Relationentheorie, Komplexitätstheorie, Ergodentheorie, Informationstheorie.[...] Für den Informatiker gewinnt die Kryptologie zusehends praktische Bedeutung, mehr und mehr gebraucht der Kryptologe die Informatik.”[12)]

[12)] [2], S. 3

Insofern sind – auch bei didaktischer Reduktion – einerseits mathematische Inhalte Lerngegenstand in einem Kryptologieunterricht. Um den Rahmen eines Wahlfaches nicht zu überschreiten, sind andererseits grundlegende mathematische Fähigkeiten Voraussetzung für diesen. Deshalb sollen nun zunächst die mathematischen Vorkenntnisse für einen erfolgreichen Kryptologieunterricht im Rahmen des Wahlfachangebots dargelegt werden. Dabei gilt unabhängig von der Schulart, dass sowohl symmetrische als auch asymmetrische Chiffrierverfahren Lehrinhalte des Kryptologieunterrichts darstellen. Denn ein Unterricht, der sich ausschließlich auf symmetrische Chiffrierverfahren beschränkt, verliert jeglichen Gegenwartsbezug und damit seine Berechtigung.

Aus den erforderlichen Vorkenntnissen erschließen sich für die einzelnen Schularten die geeigneten Jahrgangsstufen für diesen Unterricht, wobei auch auf eine fächerübergreifende Zusammenarbeit mit dem Fach Informatik geachtet wird.

5.2.1 Vorkenntnisse

Die Kryptographie ist im Wesentlichen durch zwei Bereiche geprägt: den symmetrischen und den asymmetrischen Chiffrierverfahren (vgl. Seite 4). Über die mathematischen Fähigkeiten der Grundschule hinaus, sind für diese Bereiche folgende Kenntnisse erforderlich:

Ältere symmetrische Chiffrierverfahren lassen sich auch ohne spezielle mathematische Vorkenntnisse einführen. Die Kryptanalyse basiert hier jedoch auf statistischen Verfahren, so dass die Kenntnis des Prozentbegriffs vorausgesetzt werden muss. Für Überlegungen zur perfekten Sicherheit[13)] und zur Behandlung moderner symmetrischer Verschlüsselungsverfahren ist die Kenntnis des Funktionenbegriffs notwendig.

Zur Behandlung asymmetrischer Chiffrierverfahren muss ein sicherer Umgang mit dem Funktionenbegriff vorausgesetzt werden. Daneben sind Kenntnisse über Teilbarkeitsregeln – wie die Bestimmung des größten gemeinsamen Teilers – und über Potenzen hilfreich.

Sofern die Schüler programmieren können, bietet sich die Modellierung und die Programmierung einfacher Chiffrierverfahren an. Dadurch erleben die Schüler, wie Programmierkenntnisse zur Lösung praktischer Probleme beitragen können. Das trägt zur Motivation bei und fördert durch die fächerübergreifende Arbeit mit Informatik das vernetzte Denken. Notwendige Voraussetzung für einen Kryptologieunterricht sind Programmierkenntnisse jedoch nicht.

5.2.2 Kryptologieunterricht an Hauptschulen

An Hauptschulen wird die Prozentrechnung in Jahrgangsstufe 7 und der Funktionenbegriff in Jahrgangsstufe 8 eingeführt. Ein Unterricht über symmetrische Chiffrierverfahren ist demnach an Hauptschulen bereits in der 8. Jahrgangsstufe möglich.

[13)] vgl. Vermams one–time pad auf Seite 9

Da auch asymmetrische Verschlüsselungsverfahren Lerngegenstand darstellen, erscheint ein Unterricht in Kryptologie in der Jahrgangsstufe 9 sinnvoll. Hier ist der Umgang mit Funktionen gefestigt. Ferner wird das Rechnen mit Potenzen im Mathematikunterricht der 9. Jahrgangsstufe eingeführt. Zu beachten ist hierbei, dass der Lehrplan in Mathematik der 9. Jahrgangsstufe beim Themenbereich "Potenzen und Wurzeln"

- Potenzen zur Basis 10
- Quadrieren und Radizieren

vorsieht. Durch die Beschränkung der Potenzrechnung auf Potenzen zur Basis 10 ist eine Erweiterung der Potenzrechnung auf Potenzen zu beliebigen Basen im Kryptologieunterricht erforderlich.

Da im Informatikunterricht an Hauptschulen keine Programmierkenntnisse vermittelt werden, wird auch im Wahlunterricht Kryptologie von der Erzeugung von Verschlüsselungssoftware Abstand genommen.

5.2.3 Kryptologieunterricht an Realschulen

Kenntnisse über die Prozentrechnung, Teilbarkeitsregeln und das Rechnen mit Potenzen werden im Mathematikunterricht der 5. und 6. Jahrgangsstufe eingeführt. Der Funktionenbegriff wird in der Wahlpflichtfächergruppe I in Jahrgangsstufe 8, in den Wahlpflichtfächergruppen II und III zu Beginn der 9. Jahrgangsstufe vermittelt.

Folglich beschränkt sich ein Wahlunterricht in Kryptologie unabhängig von der Wahlpflichtfächergruppe auf die Jahrgangsstufen 9 und 10.

Grundlagen der Programmierung werden an Realschulen in der Wahlpflichtfächergruppe I zu Beginn der 10. Jahrgangsstufe vermittelt. Sofern ein Unterricht in Kryptologie in der 10. Jahrgangsstufe angeboten wird, kann folglich auch die Erstellung von Verschlüsselungssoftware in den Kryptologieunterricht eingebaut werden. Der im nächsten Kapitel folgende Lehrplan sieht diesbezüglich Möglichkeiten zur inneren Differenzierung im Unterricht vor.

5.2.4 Kryptologieunterricht an Gymnasien

Analog zum Lehrplan für Realschulen werden Teilbarkeitsregeln, die Prozentrechnung und das Rechnen mit Potenzen im Mathematikunterricht der 5. und 6. Jahrgangsstufe vermittelt. Funktionen werden an Gymnasien in der Jahrgangsstufe 8 behandelt. Insofern kann Kryptologie an Gymnasien für Schüler der Jahrgangsstufen 9 bis 12 angeboten werden.

Berücksichtigt man auch Kenntnisse in der Programmierung, empfiehlt sich Kryptologie für Schüler ab der 10. Jahrgangsstufe. Denn am naturwissenschaftlich–technologischen Gymnasium lernen Schüler der 9. Jahrgangsstufe die imperative Programmierung kennen. Der im nächsten Kapitel vorgestellte Lehrplan sieht deshalb Möglichkeiten zur Erstellung von Verschlüsselungssoftware im Rahmen der inneren Differenzierung vor.

5.2.5 Zusammenfassung

Wenn Kryptologie im Rahmen des Wahlfachangebotes an Schulen Eingang finden soll, sind bestimmte Vorkenntnisse aus anderen Unterrichtsfächern erforderlich. Deshalb kann Kryptologie an Hauptschulen in der 9. Jahrgangsstufe unterrichtet werden. Aufgrund fehlender mathematischer Vorkenntnisse, sind auch mathematische Inhalte wie z. B. die Potenzrechnung im Kryptologieunterricht zu vermitteln.

Schüler an Realschulen und Gymnasien verfügen nach der 8. Jahrgangsstufe über die mathematischen Vorkenntnisse, um sowohl historische Aspekte der Kryptologie als auch die aktuellen Chiffrierverfahren verstehen und anwenden zu können. Zur Förderung der Schüler, die über Programmierkenntnisse verfügen, sind im folgenden Lehrplan Möglichkeiten zur Erstellung von Verschlüsselungssoftware im Rahmen der inneren Differenzierung vorgesehen.

5.3 Organisation eines Unterrichts in Kryptologie

Wie im vorhergehenden Kapitel erläutert, kann Kryptologie aufgrund des erforderlichen Vorwissens an allen allgemeinbildenden Schulen in der Jahrgangsstufe 9 und aufwärts unterrichtet werden. Für diese Schulen folgt nun eine zeitliche Grobplanung des Unterrichts in Kryptologie.

Anschließend werden für jede Schulart Lehrpläne in Kryptologie vorgestellt. Hierfür werden Lerninhalte ausgewählt, in eine zeitliche Abfolge gebracht und die jeweils benötigte Unterrichtszeit abgeschätzt.

5.3.1 Zeitliche Grobstruktur

Für einen Unterricht in Kryptologie werden im Folgenden zwei Wochenstunden für ein Schuljahr vorgesehen. Alternativ kann ein Unterricht in Kryptologie über zwei Jahre hinweg einstündig gestaltet werden.

Der Lehrplan geht bei einem 2-stündigen Unterrichtsfach von 56 Unterrichtsstunden im Jahr aus. Die folgende Beschreibung der Lehrinhalte ist so gestaltet, dass in dieser Zeit nicht nur ein Überblick über symmetrische und asymmetrische Chiffrierverfahren vermittelt werden kann. Es wird auch berücksichtigt, zeitaufwendigere Unterrichtsmethoden wie z. B. entdeckenlassende und erarbeitende Unterrichtsformen einzusetzen, damit ein ganzheitliches Lernen, d. h. ein Lernen mit Kopf, Herz und Hand möglich wird.

Daneben werden Hinweise zum Einsatz von Ver- und Entschlüsselungssoftware gegeben. Sofern Programmierkenntnisse vorhanden sind, können einfache Chiffrieralgorithmen auch selbst erstellt werden. Damit sich die Stundenzahl dadurch nicht erhöht, werden Wahlpflichtbereiche vorgegeben, aus denen bestimmte Themen umzusetzen sind.

5.3.2 Lerninhalte für einen Unterricht in Kryptologie

Im Folgenden werden Lehrpläne für einen Wahlunterricht Kryptologie vorgestellt. An Hauptschulen ist dabei auf eine anschauliche Präsentation unter Einbeziehung vieler Beispiele zu achten. Fehlende mathematische Vorkenntnisse über die Potenzrechnung werden durch entsprechende Lerninhalte im Bereich der asymmetrischen Chiffrierverfahren behoben. Da Programmierkenntnisse an Hauptschulen nicht vorausgesetzt werden können, sieht der Lehrplan auch keinen Einsatz entsprechender Verschlüsselungssoftware vor.

Da Schüler an Realschulen und Gymnasien über ähnliche Vorkenntnisse und eine vergleichbare Auffassungsgabe verfügen, werden an beiden Schularten dieselben Lerninhalte vorgesehen und damit derselbe Lehrplan verwendet. Um Schüler mit Programmierkenntissen die Erstellung von Verschlüsselungssoftware im Unterricht zu ermöglichen, sind an geeigneten Stellen im Lehrplan Wahlpflichtbereiche vorgesehen. Aus diesen können die Schüler jeweils ein Thema entsprechend ihres Kenntnisstandes und ihrer Neigung im Rahmen der inneren Differenzierung wählen.

5.3.2.1 Lerninhalte von Kryptologie an Hauptschulen

1. Grundlagen (ca. 8 Stunden)
Die Schüler lernen die Notwendigkeit der Datenverschlüsselung anhand von Beispielen aus dem Alltag kennen. Zum Aufbau einer Fachsprache werden grundlegende Fachbegriffe aus der Kryptologie erläutert und an Beispielen veranschaulicht. Ferner lernen die Schüler die Verschlüsselung als Relation kennen, die einen Klartext in einen Geheimtext überführt. Die Kryptographie wird zur Steganographie, d. h. zum Verbergen von Nachrichten abgegrenzt und als “offene” Geheimschrift hervorgehoben.

- Notwendigkeit der Verschlüsselung und des Datenschutzes; Beispiele aus dem Alltag (z. B. Homebanking, Pay–TV)
- Begriffsbestimmungen: Klärung und Veranschaulichung kryptologischer Fachbegriffe (z. B. Kryptographie, Kryptanalyse, Kryptologie, Chiffrieren, Dechiffrieren, Schlüssel); Abgrenzung der Kryptanalyse zu unerlaubten Angriffen auf Computersysteme
- Verschlüsselung als Relation; Einführung von Klar- und Geheimtextalphabeten
- Steganographie als verwandte Wissenschaft
  - Beispiele für Steganographie (z. B. Geheimtinte, versteckte Botschaften in Bildern; Beispiele aus der Antike)
  - Abgrenzung zur Kryptographie
  - Erstellen und Verbergen eigener Geheimbotschaften

2. Symmetrische Chiffrierverfahren

Monoalphabetische Substitution (ca. 12 Stunden)
Ausgehend von leicht durchschaubaren Geheimschriften der Bi- und Ror–Sprache lernen die Schüler erste Verschlüsselungen aus der Geschichte durch verschobene Alphabete kennen. Aus den Schwächen der Caesar–Chiffre wird die Monographische Substitution hergeleitet. Die Schüler erkennen, dass durch die Buchstabenhäufigkeit eine Kryptanalyse ermöglicht wird und nehmen selbst Entschlüsselungen vor. Daraus wird deutlich, dass durch Verschleierung der Einzelzeichenhäufigkeit die Sicherheit eines Kryptogramms erhöht werden kann.

- Geheimsprachen durch Veränderung von Silben oder Vokalen (Bi–Sprache, Ror–Sprache); Beispiele aus der Literatur (z. B. Joachim Ringelnatz: Bi–Gedicht, Astrid Lindgren: Ror–Sprache aus "Kalle Blomquist lebt gefährlich")
- Caesar–Verschiebechiffre
  - Einführung, Anwendung und Variation des Schlüssels
  - Kryptanalyse durch systematisches Durchprobieren aller Verschiebemöglichkeiten
  - Basteln einer Chiffrierscheibe (Hinweis auf Leon Battista Alberti)
- Monographische Substitution:
  - Einzelzeichen werden durch Einzelzeichen ersetzt: Einführung durch Verallgemeinerung der Caesar–Chiffre; Kryptanalyse anhand der Buchstabenhäufigkeit
  - Entschlüsselung eines monographischen Kryptogramms aus der Literatur (z. B. Edgar Allan Poe: "Der Goldkäfer"; Arthur Conan Doyles: "Die tanzenden Männchen")
  - Einzelzeichen werden durch mehrere Geheimtextzeichen ersetzt: Herausarbeitung anhand der Schwächen der Einzelzeichen–Chiffrierung; Überlegungen zur Sicherheit

Transposition (ca. 4 Stunden)
Die Schüler lernen die Transposition als ein Verfahren kennen, das die Position der Buchstaben im Klartext verändert, ohne die Klartextbuchstaben selbst durch andere Zeichen zu ersetzen. Dadurch lernen sie, die Chiffrierverfahren der Transposition und der Substitution zu unterscheiden.

- Einführung der Transposition anhand von Beispielen (z. B. Transposition durch eine Schablone, mithilfe einer Matrix)
- Überlegungen zur Sicherheit dieser Verfahren
- Abgrenzung zur Substitution

Polyalphabetische Substitution (ca. 10 Stunden)
Anhand der Vigenère–Verschlüsselung lernen die Schüler die polyalphabetische Substitution als ein Verfahren kennen, bei dem ein Wechsel der Chiffrierschritte stattfindet. In der Kryptanalyse wird der Kasiski–Test hergeleitet und von den Schülern durchgeführt. Ferner lernen die Schüler die Enigma als eine polyalphabetische Chiffriermaschine kennen.

- Abgrenzung zur monoalphabetischen Substitution
- Vigenère–Verschlüsselung
- Kryptanalyse: Herleitung des Kasiski–Tests durch Plausibilitätsüberlegungen; Anwendung des Kasiski–Tests
- Erhöhung der Sicherheit durch extrem lange Schlüssel (Schlüsselwürmer)
- Die Enigma: Aufbau und Funktionsweise der Enigma; geschichtlicher Hintergrund

Perfekte Sicherheit (ca. 4 Stunden)
Bei der Verschlüsselung nach Gilbert S. Vernam wird nun durch Plausibilitätsüberlegungen deutlich, dass unendlich lange Schlüssel aus Zufallszahlen perfekte Sicherheit gewährleisten.

- Vernams one–time pad: Verschlüsselung nach Vernam
- Perfekte Sicherheit der Vernam–Chiffre (Plausibilitätsüberlegungen)
- Nachteile der Chiffre

3. Asymmetrische Chiffrierverfahren (ca. 12 Stunden)

Die Schüler lernen asymmetrische Chiffrierverfahren als Verfahren ohne Schlüsselaustausch kennen. Hierzu werden private und öffentliche Schlüssel eingeführt und anhand dieser, die asymmetrische Verschlüsselung veranschaulicht. Auf diese Weise erfolgt eine klare Abgrenzung zur symmetrischen Verschlüsselung. Als Beispiel einer asymmetrischen Verschlüsselung wird das RSA–Verfahren vorgeführt und an ausgewählten Beispielen angewandt.

- Abgrenzung der asymmetrischen Verschlüsselung zu symmetrischen Verfahren
- Modulo–Rechnung
- Einweg–Funktionen: Beispiele und Notwendigkeit der Einweg–Funktionen
- Rechnen mit Potenzen
- Primzahlen: Kennzeichen; Auffinden von Primzahlen (Sieb des Eratosthenes)
- Umwandlung von Buchstaben in Zahlen (z. B. ASCII–Code)
- RSA–Chiffrierung: Verfahren der RSA–Verschlüsselung anhand von Beispielen; Entschlüsselung RSA–chiffrierter Kryptogramme
- Überlegungen zur Sicherheit des RSA–Verfahrens

4. Authentizität (ca. 6 Stunden)
Die Schüler erkennen die Notwendigkeit, Authentizität von Nachrichten und Benutzern zu überprüfen. Zur Überprüfung der Nachrichtenauthentizität erlernen die Schüler das Vorgehen zur Erstellung einer elektronischen Unterschrift im Rahmen des RSA–Verfahrens. Bezüglich der

Benutzerauthentizität werden die Möglichkeiten mithilfe von Passwörten und Chipkarten erlernt.

- Nachrichtenauthentizität: Signieren einer Nachricht (elektronische Unterschrift) mit dem RSA–Verfahren
- Benutzerauthentizität:
  - Passwortverfahren
  - Challenge–and–Response

5.3.2.2 Lerninhalte von Kryptologie an Realschulen und Gymnasien

1. Grundlagen (ca. 6 Stunden)
Die Schüler lernen die Notwendigkeit der Datenverschlüsselung anhand von Beispielen aus dem Alltag kennen. Zum Aufbau einer Fachsprache werden grundlegende Fachbegriffe aus der Kryptologie erläutert und an Beispielen veranschaulicht. Ferner lernen die Schüler die Verschlüsselung als Relation kennen, die einen Klartext in einen Geheimtext überführt. Die Kryptographie wird zur Steganographie, d. h. zum Verbergen von Nachrichten (z. B. durch Geheimtinte) abgegrenzt und als "offene" Geheimschrift hervorgehoben.

- Notwendigkeit der Verschlüsselung und des Datenschutzes; Beispiele aus dem Alltag (z. B. Homebanking, Pay–TV)
- Begriffsbestimmungen: Klärung und Veranschaulichung kryptologischer Fachbegriffe (z. B. Kryptographie, Kryptanalyse, Kryptologie, Chiffrieren, Dechiffrieren, Schlüssel); Abgrenzung der Kryptanalyse zu unerlaubten Angriffen auf Computersysteme
- Verschlüsselung als Relation; Einführung von Klar- und Geheimtextalphabeten
- Steganographie als verwandte Wissenschaft: Abgrenzung zur Kryptographie; Beispiele der Steganographie früher und heute; Erstellen und Verbergen eigener Geheimbotschaften

2. Symmetrische Chiffrierverfahren

Monoalphabetische Substitution (ca. 12 Stunden)
Ausgehend von leicht durchschaubaren Geheimschriften der Bi- und Ror–Sprache lernen die Schüler erste Verschlüsselungen aus der Geschichte durch verschobene Alphabete kennen. Aus den Schwächen der Caesar–Chiffre wird die monographische Substitution hergeleitet. Bei der Kryptanalyse aufgrund der Buchstabenhäufigkeit kann im Gymnasium an den Mathematikunterricht der Jahrgangsstufe 6 (Relative Häufigkeit) angeknüpft werden. Die Schüler erkennen, dass die Sicherheit eines Kryptogramms durch Verschleierung der Einzelzeichenhäufigkeit erhöht werden kann. Ferner lernen die Schüler die polygraphische Substitution anhand eines Beispiels aus der Geschichte der Kryptographie kennen.

- Geheimsprachen durch Veränderung von Silben oder Vokalen (Bi–Sprache, Ror–Sprache); Beispiele aus der Literatur (z. B. Joachim Ringelnatz: Bi–Gedicht, Astrid Lindgren: Ror–Sprache aus “Kalle Blomquist lebt gefährlich”)
- Caesar–Verschiebechiffre
  - Einführung, Anwendung und Variation des Schlüssels; Kryptanalyse durch systematisches Durchprobieren aller Verschiebemöglichkeiten
  - Wahlpflichtbereich: Eines aus folgenden Themen ist im Unterricht zu behandeln.
    * Basteln einer Chiffrierscheibe (Hinweis auf Leon Battista Alberti)
    * Erstellung einer Verschlüsselungssoftware nach der Caesar–Chiffre
    * Anwendung und Analyse der Verschlüsselungssoftware ROT13
- Monographische Substitution:
  - Einzelzeichen werden durch Einzelzeichen ersetzt: Einführung durch Verallgemeinerung der Caesar–Chiffre; Kryptanalyse anhand der Buchstabenhäufigkeit
  - Einzelzeichen werden durch mehrere Geheimtextzeichen ersetzt: Herausarbeitung anhand der Schwächen der Einzelzeichen–Chiffrierung; Hinweis auf Kryptanalyse durch Häufigkeitsverteilung von Bigrammen
  - Wahlpflichtbereich: Eines aus folgenden Themen ist im Unterricht zu behandeln.
    * Erstellung einer monographischen Verschlüsselungssoftware
    * Entschlüsselung eines monographischen Kryptogramms aus der Literatur (z. B. Edgar Allan Poe: “Der Goldkäfer”; Arthur Conan Doyles: “Die tanzenden Männchen”)
    * Analyse der Geheimschrift von Maria Stuart; geschichtlicher Hintergrund und Folgen der Entschlüsselung
- Polygraphische Substitution
  - Wahlpflichtbereich: Eines aus folgenden Themen ist im Unterricht zu behandeln.
    * Playfair–Verfahren: Einführung und Anwendung; Sicherheitsüberlegungen
    * Delastelle–Verfahren: Einführung und Anwendung; Sicherheitsüberlegungen
  - Codes: Beispiele; Anwendungen aus der Geschichte; Sicherheit

Transposition (ca. 2 Stunden)
Die Schüler lernen die Transposition als ein Verfahren kennen, das die Position der Buchstaben im Klartext verändert, ohne die Klartextbuchstaben selbst durch andere Zeichen zu ersetzen. Auf diese Weise lernen sie, die Chiffrierverfahren der Transposition und der Substitution zu unterscheiden.

- Einführung der Transposition anhand von Beispielen (z. B. Transposition durch eine Schablone, mithilfe einer Matrix); Überlegungen zur Sicherheit dieser Verfahren
- Abgrenzung zur Substitution
- Wahlpflichtbereich: Eines aus folgenden Themen ist im Unterricht zu behandeln.
  - Erstellung einer Verschlüsselungssoftware durch Transposition
  - Transposition der Spartaner mit Hilfe der Skytale; Basteln einer Skytale

Polyalphabetische Substitution (ca. 10 Stunden)
Anhand der Vigenère–Verschlüsselung lernen die Schüler die polyalphabetische Substitution als ein Verfahren kennen, bei dem ein Wechsel der Chiffrierschritte stattfindet. In der Kryptanalyse wird der Kasiski–Test hergeleitet und von den Schülern durchgeführt. Ferner besteht die Möglichkeit, dass die Schüler die Enigma als eine polyalphabetische Chiffriermaschine kennen lernen.

- Abgrenzung zur monoalphabetischen Substitution
- Vigenère–Verschlüsselung
- Kryptanalyse: Herleitung des Kasiski–Tests durch Plausibilitätsüberlegungen; Anwendung des Kasiski–Tests
- Wahlpflichtbereich: Eines aus folgenden Themen ist im Unterricht zu behandeln.
  - Erstellung einer Verschlüsselungssoftware nach der Vigenère–Verschlüsselung
  - Die Enigma: Aufbau und Funktionsweise der Enigma; geschichtlicher Hintergrund

Perfekte Sicherheit (ca. 4 Stunden)
Anhand der Überlegungen zum Kasiski–Test erkennen die Schüler eine Erhöhung der Sicherheit der Vigenère–Verschlüsselung durch extrem lange Schlüssel (Schlüsselwürmer). Bei der Verschlüsselung nach Gilbert S. Vernam wird nun durch Plausibilitätsüberlegungen deutlich, dass unendlich lange Schlüssel aus Zufallszahlen perfekte Sicherheit gewährleisten. Aufgrund der Realitätsnähe und zur Vorbereitung auf praxisrelevante Chiffrierverfahren, wird die Vernam–Chiffre im Dualsystem behandelt.

- Buchstaben als Dualzahlen: Aufbau des Dualsystems; Rechnen mit Dualzahlen; ASCII–Code der Buchstaben
- Vernams one–time pad: Verschlüsselung nach Vernam; Erkenntnis der perfekten Sicherheit der Vernam–Chiffre durch Plausibilitätsüberlegungen; Nachteile der Chiffre
- Problem der Erzeugung von Zufallszahlen; praktische Lösungsansätze

Praxisrelevante monoalphabetische Chiffrierung (ca. 2 Stunden)
Die Schüler lernen anhand der DES–Verschlüsselung ein modernes und praxisrelevantes monoalphabetisches Chiffrierverfahren kennen. Auf diese Weise erkennen die Schüler die Bedeutung und die Einsatzbereiche monoalphabetischer Verschlüsselungen.

- Schema der DES–Verschlüsselung

- Einsatzbereiche
- Sicherheit

3. Asymmetrische Chiffrierverfahren (ca. 12 Stunden)

Die Schüler lernen asymmetrische Chiffrierverfahren (Public–Key–Kryptographie) als ein Verfahren ohne Schlüsselaustausch durch die Unterscheidung in private und öffentliche Schlüssel kennen. Auf diese Weise erfolgt eine klare Abgrenzung zur symmetrischen Verschlüsselung. Als Beispiel einer asymmetrischen Verschlüsselung wird das RSA–Verfahren behandelt. Beweise zum RSA–Verfahren können je nach Leistungsfähigkeit der Schüler durchgeführt werden. Praktische Anwendung asymmetrischer Verfahren erfahren die Schüler anhand der PGP–Verschlüsselung.

- Abgrenzung asymmetrischer Verschlüsselung zu symmetrischen Verfahren
- Modulo–Rechnung
- Einweg–Funktionen: Beispiele und Notwendigkeit der Einweg–Funktionen
- Diffie–Hellman–Schlüsselaustausch
- RSA–Chiffrierung: Verfahren der RSA–Verschlüsselung (Beweis bzw. Plausibilitätsüberlegungen); Verschlüsselung einfacher Texte; Entschlüsselung RSA–chiffrierter Kryptogramme
- Primzahlen: Auffinden von Primzahlen (Sieb des Eratosthenes)
- Sicherheit des RSA–Verfahrens (Einsatz einer Algebra–Software)
- PGP–Chiffrierung als Beispiel einer hybriden Verschlüsselung; Einrichtung von PGP am PC und Anwendung

4. Authentizität und Integrität (ca. 8 Stunden)

Die Schüler erkennen die Notwendigkeit, Authentizität von Nachrichten und Benutzern sowie Integrität von Nachrichten überprüfen zu können. Sie lernen Methoden zur Überprüfung der Authentizität und Integrität im Rahmen der Public–Key–Kryptographie kennen. Im Rahmen dieses Themas eignet sich der Einsatz des Signaturgesetzes im Unterricht.

- Nachrichtenauthentizität: Signieren einer Nachricht (elektronische Unterschrift) mit dem RSA–Verfahren; praktische Einsätze der elektronischen Signatur (Signaturgesetz)
- Nachrichtenintegrität: Notwendigkeit; Lösungsansätze zur Gewährleistung der Nachrichtenintegrität
- Benutzerauthentizität:
  - Passwortverfahren

- Challenge–and–Response
- Zero–Knowledge–Verfahren

5.3.3 Zusammenfassung

Um kryptologische Inhalte umfassend und ohne Zeitdruck vermitteln zu können, werden für einen Unterricht in Kryptologie zwei Wochenstunden für ein Schuljahr vorgesehen. Daran knüpft der anschließend vorgestellte Lehrplan in Kryptologie an. Für jede Schulart sind dabei Lerninhalte aus den Bereichen

- Grundlagen der Kryptologie
- Symmetrische Chiffrierverfahren
- Asymmetrische Chiffrierverfahren
- Authentizität und Integrität

vorgesehen.

Zu beachten sind im Lehrplan für Realschulen und Gymnasien Wahlpflichtbereiche, aus denen jeweils ein Thema ausgewählt werden soll. Auf diese Weise wird eine innere Differenzierung zwischen Schülern mit und ohne Programmierkenntnissen erleichtert.

6 Unterrichtsbeispiele

Nachdem im vorhergehenden Kapitel die Lerninhalte für einen Unterricht in Kryptologie festgelegt wurden, folgen nun Unterrichtsbeispiele zur Umsetzung ausgewählter Lernziele. Diese Beispiele sind dabei möglichst allgemein gehalten und dienen lediglich als Grobstruktur für einen Unterricht, der im Einzelnen auf die anthropologisch–psychologischen sowie auf die sozial–kulturellen Voraussetzungen der jeweiligen Lerngruppe ausgerichtet werden muss.

Analog zur Berliner Didaktik – auch als lehr- und lerntheoretische Didaktik bezeichnet – beziehen sich die anthropologisch–psychologischen Bedingungen auf den Entwicklungsstand der Lernenden, ihr entsprechendes Leistungsvermögen sowie auf die Lehrfähigkeit und -bereitschaft der Lehrkraft. Sozial–kulturelle Voraussetzungen legen Gegebenheiten wie Vorwissen, Interessen, soziale Herkunft und Zusammensetzung der Lerngruppe, sowie die finanzielle Ausstattung der Schule fest.

Nach der Berliner Didaktik hat eine Lehrkraft zur Durchführung eines Unterrichts Entscheidungen über Intentionen, Inhalte, Methoden und Medien zu treffen.

Intentionen/Inhalte:
: Da heute in der Didaktik der Grundsatz vorherrscht, dass “alle Aspekte des Unterrichtsprozesses und alle Momente der Unterrichtsplanung einer ’allgemeinen Zielorientierung’ unterliegen”[1)], werden zunächst die Intentionen jeder Unterrichtseinheit festgelegt. Anschließend werden die Inhalte aufgestellt, mit denen die gewünschten Lernziele erreicht werden können.

Methoden/Medien:
: Da hier einerseits nur eine Grobstruktur für einen Unterricht in Kryptologie vorgestellt werden soll und andererseits methodische Entscheidungen sehr stark von der Lerngruppe abhängen, wird auf die Methodik zumeist nicht eingegangen. Aufgrund der starken Interdependenz von Methoden und Medien, wird damit auch die Medienauswahl der einzelnen Lehrkraft überlassen und hier nicht bestimmt.

6.1 Grundlagen

Wie bereits aus dem im vorhergehenden Kapitel vorgestellten Lehrplan ersichtlich ist, soll im Themengebiet “Grundlagen” die Notwendigkeit der Kryptographie erkannt, Fachbegriffe zum

[1)] vgl. [19], S. 196

Aufbau einer Fachsprache eingeführt und die Kryptographie zur Steganographie abgegrenzt werden.

6.1.1 Notwendigkeit der Kryptographie

Intentionen
Die Notwendigkeit der Datenverschlüsselung wird durch die Herausarbeitung der Ziele der Kryptographie besonders deutlich. Zusätzlich erhalten die Schüler dadurch Anhaltspunkte, um später zu erlernende Chiffrierverfahren im Hinblick auf ihren praktischen Nutzen beurteilen zu können. Aus Gründen der Motivation und einer besseren Behaltensleistung sind die Ziele der Kryptographie durch Beispiele aus der Praxis zu veranschaulichen.

Damit ergeben sich folgende Lernziele:

- Die Schüler sollen in der Lage sein, die Hauptziele der modernen Kryptographie angeben zu können.
- Die Schüler sollen anhand dieser Ziele die Notwendigkeit kryptographischer Methoden erkennen.
- Den Schülern soll der Einsatz kryptographischer Methoden in der Praxis anhand von Beispielen aus dem Alltag bewusst werden.

Inhalte
Als Ziele der Kryptographie werden

1. die Vertraulichkeit einer Nachricht,
2. die Integrität einer Nachricht,
3. die Authentizität und
4. die Verbindlichkeit (Nichtabstreitbarkeit) der Sendung einer Nachricht

angesehen.

Zur Heranführung an das erste Ziel kann der Lehrer zeigen, dass er als Systemadministrator sämtliche E-Mails der Schüler im Netzwerk der Schule lesen kann. Sollten folglich Schüler per E-Mail solche Nachrichten austauschen, die der Lehrer nicht lesen darf, müssen diese verschlüsselt werden. Weitere Beispiele, bei denen die Vertraulichkeit einer Nachricht wichtig erscheint, sind der Nachrichtenaustausch in Kreisen der Diplomatie, des Militärs und der Geheimdienste.

Die Notwendigkeit der Nachrichtenintegrität wird an folgendem Beispiel deutlich: Bob schickt an Alice eine Postkarte mit der Nachricht: “Ich liebe dich”. Ein unbefugter Dritter (z. B. der ältere Bruder von Alice) nimmt nach der Zustellung die Postkarte an sich, verändert die Nachricht zu “Ich liebe dich nicht” und wirft die Karte wieder in Alice Briefkasten. Ein anderes Beispiel ist, dass E-Mails an Routern im Internet leicht abgefangen und verändert werden können. Durch Verschlüsselung wird die Nachricht für einen unbefugten Dritten nicht nur unleserlich, sie verhindert auch das unbemerkte Verändern einer Nachricht. Daneben existieren gesonderte

kryptographische Methoden, mit denen festgestellt werden kann, ob eine Nachricht verändert wurde.

Zur Authentizität gehört sowohl die Identifikation des Kommunikationspartners (Teilnehmerauthentizität), als auch der Nachweis, dass die Nachricht tatsächlich vom angegebenen Absender stammt (Nachrichtenauthentizität).

Teilnehmerauthentizität:
Die Identifizierung einer Person kann grundsätzlich auf drei Weisen erfolgen:

- Die Identität einer Person kann durch biologische Merkmale wie z. B. den Fingerabdruck oder eine händische Unterschrift nachgewiesen werden.
- Die Identität einer Person kann durch den Besitz z. B. eines Schlüssels oder eines Ausweises nachgewiesen werden.
- Die Identität einer Person kann durch Wissen z. B. eines Passwortes nachgewiesen werden.

Die Kryptographie befasst sich hier vor allem mit der Authentifizierung des Kommunikationspartners durch geheimes Wissen – wie z. B. durch Angabe von PIN und TAN (Transaktionsnummer) bei Überweisungen im Rahmen des Homebanking – aber auch mit kombinierten Methoden der Authentifizierung. Zum Beispiel benötigt man bei Geldausgabeautomaten sowohl eine Bankkarte (Besitz) als auch die zugehörige PIN (Wissen) um auf ein Konto zugreifen zu können. Daneben sollten auch die Methoden angesprochen werden, wie beim Pay-TV, in Mobilfunknetzen oder beim Digital Rights Management (DRM) die Identität des Kommunikationspartners und damit die Berechtigung zur Benutzung überprüft wird.

Nachrichtenauthentizität:
Zur Einführung in die Problematik der Nachrichtenauthentizität kann im Unterricht z. B. gezeigt werden, dass durch Angabe einer falschen Absenderadresse in einer E-Mail der Kommunikationspartner getäuscht werden kann. Dies ist nicht möglich, wenn die Nachricht mit einer elektronischen Unterschrift (Signatur) versehen ist, die im Bereich der Public–Key–Kryptographie entwickelt wird.

Schließlich soll über kryptologische Verfahren eine Verbindlichkeit beim Nachrichtenaustausch erreicht werden. Als Beispiel kann angeführt werden, dass beim elektronischen Handel über das Internet (E-Commerce) die Abwicklung des Geschäfts nicht abgestritten werden darf.

6.1.2 Begriffsbestimmungen

Intentionen
Zum Aufbau einer Fachsprache gehört nicht nur das Wissen um die Bedeutung wichtiger Begriffe aus der Kryptologie; deren Verwendung muss auch zur Gewohnheit werden.

Lernziele sind folglich:

- Die Schüler sollen die Bedeutung wichtiger kryptologischer Fachbegriffe kennen.
- Die Schüler sollen Fachbegriffe aus der Kryptologie korrekt anwenden können.

Inhalte
Zum Erreichen oben genannter Lernziele eignen sich folgende Begriffsbestimmungen:

- Kryptographie ist die Wissenschaft von der Verschlüsselung von Daten und der Entwicklung von Verschlüsselungsverfahren.
- Kryptanalyse (bzw. Kryptoanalyse) ist die Wissenschaft von der Entschlüsselung von Daten ohne Kenntnis des Schlüssels. Ziel ist die Analyse von Schwachstellen kryptologischer Verfahren[2)].
- Kryptologie ist die Zusammenfassung von Kryptographie und Kryptanalyse.
- Klartext ist die Bezeichnung für eine unverschlüsselte Nachricht.
- Klartextalphabet ist der Zeichenvorrat, mit dessen Hilfe der Klartext formuliert wird.
- Geheimtext oder Kryptogramm ist die Bezeichnung für eine verschlüsselte Nachricht.
- Geheimtextalphabet ist der Zeichenvorrat, mit dessen Hilfe der Geheimtext formuliert wird.
- Chiffrieren bzw. Verschlüsseln ist der Vorgang, bei dem ein Klartext mittels eines bestimmten Verfahrens (Algorithmus) in einen Geheimtext umgewandelt wird.
- Dechiffrieren bzw. Entschlüsseln ist die Umwandlung eines Geheimtextes zurück in den Klartext.

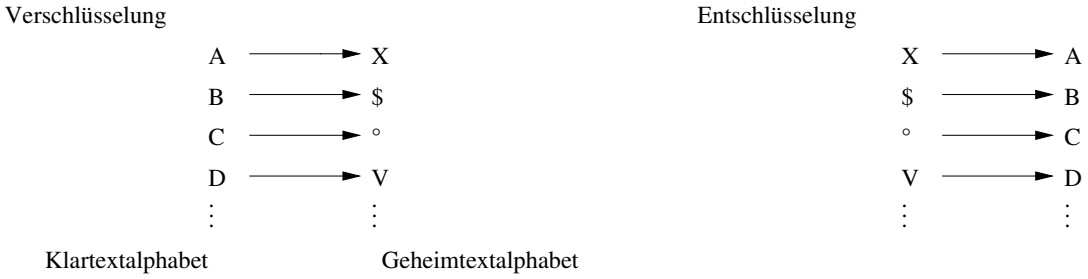


Abbildung 6.1: Beispiel einer Verschlüsselung mit zugehöriger Entschlüsselung

Anhand der Abbildung 6.1 wird deutlich, dass die Verschlüsselung eine Relation darstellt, die einen Klartext in einen Geheimtext überführt. Die Entschlüsselung stellt die Umkehrrelation zur Verschlüsselungsrelation dar. Damit die Entschlüsselung eindeutig ist, muss die Umkehrrelation jedem Geheimtextzeichen genau ein Klartextzeichen zuordnen (vgl. Abbildung 6.2).

Jede Verschlüsselung beruht auf einem Schlüssel, der angibt, wie das Verschlüsselungsverfahren in einer bestimmten Situation anzuwenden ist (vgl. Abbildung 6.3).

[2)] Wichtig ist an dieser Stelle eine klare Abgrenzung zu illegalen Angriffen auf fremde Computersysteme.

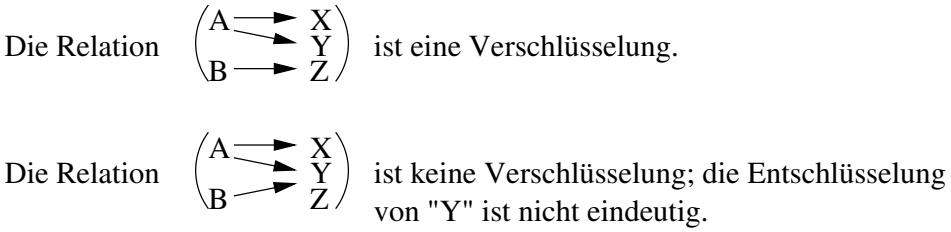


Abbildung 6.2: Beispiel für eine eindeutig umkehrbare und eine nicht eindeutig umkehrbare Verschlüsselung.

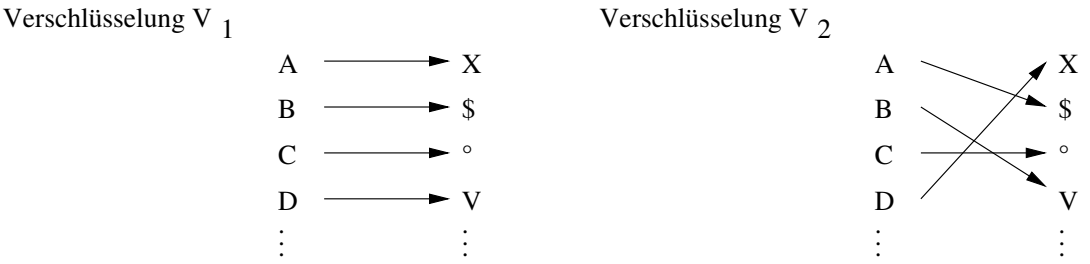


Abbildung 6.3: Verschlüsselungsverfahren werden durch den Schlüssel 1 bzw. 2 bestimmt.

Anmerkung:
In dieser Arbeit wird zwischen Code und Chiffren unterschieden. Chiffren legen eine Abbildungsvorschrift zur Verschlüsselung von Nachrichten fest. Ein Code stellt eine Abbildungsvorschrift dar, die z. B. Schriftzeichen für die Datenverarbeitung in Zahlen umwandelt (z. B. ASCII–Code). Mittels Chiffren wird folglich die Geheimhaltung einer Nachricht angestrebt, während mit einem Code die Nachricht zur Übertragung oder Weiterverarbeitung umgewandelt wird. Entsprechend gilt auch die Unterscheidung der Begriffe chiffrieren und codieren bzw. dechiffrieren und decodieren.

6.1.3 Steganographie

Intentionen
Um die Kryptographie als Wissenschaft vollständig zu erfassen, gehört auch ein Exkurs über die Steganographie als verwandte Wissenschaft zu den Lerninhalten; denn beide Forschungsgebiete haben zum Ziel, eine Botschaft vor unbefugten Dritten zu schützen. Da allerdings die Kryptographie von einem völlig anderen Ansatz ausgeht, ist es wichtig, auf die unterschiedlichen Intentionen einzugehen und Methoden der Kryptographie von denen der Steganographie zu distanzieren.

Um sowohl die Gemeinsamkeiten als auch Unterschiede zwischen Kryptographie und Steganographie herauszuarbeiten, bietet sich eine gründliche, aber nicht zu detaillierte Behandlung der Steganographie an. Neuere Methoden bleiben daher unberücksichtigt. Als Lernziele ergeben sich damit:

- Die Schüler sollen Methoden der Kryptographie von denen der Steganographie abgrenzen können.
- Die Schüler sollen Methoden der linguistischen und der technischen Steganographie kennen lernen und Beispiele beiden Kategorien zuordnen können.
- Die Schüler sollen Vor- und Nachteile der Steganographie erkennen.

Inhalte
Zur Einführung in die Steganographie sollte zunächst der bereits behandelte Begriff der Kryptographie wiederholt und erläutert werden. In der Kryptographie werden die durch entsprechende Verfahren verschlüsselten Nachrichten über unsichere Wege an den Empfänger geschickt. Dadurch wird nicht nur der Austausch von Nachrichten offensichtlich; unbefugte Dritte können das Kryptogramm in der Regel leicht abfangen. Ob diese auch Zugang zur Nachricht erhalten, ist allein von der Sicherheit des verwendeten kryptographischen Verfahrens abhängig.

In der Steganographie wird versucht, eine Nachricht an den Empfänger dadurch geheim zu halten, dass die Existenz der Nachricht selbst verheimlicht wird. Ihr Ziel ist es, den Nachrichtenaustausch vor unbefugten Dritten zu verbergen.

Der Unterschied zwischen Kryptographie und Steganographie wird an folgendem Beispiel besonders deutlich: Ein Häftling möchte aus dem Gefängnis eine geheime Nachricht (z. B. über den Zeitpunkt seines Ausbruchsversuchs) einem Komplizen auf freiem Fuß zukommen lassen. Die Methoden der Kryptographie wären hier nicht geeignet, denn eine unleserliche Nachricht würde Misstrauen erwecken und damit die Sicherheitskontrollen nicht passieren. Der Inhaftierte wird folglich versuchen, die geheime Nachricht in einem harmlos erscheinenden Brief zu verstecken; d. h. er bedient sich der Steganographie.

In der Steganographie lassen sich zwei Forschungsgebiete unterscheiden: die technische und die linguistische Steganographie (vgl. Abbildung 6.4).

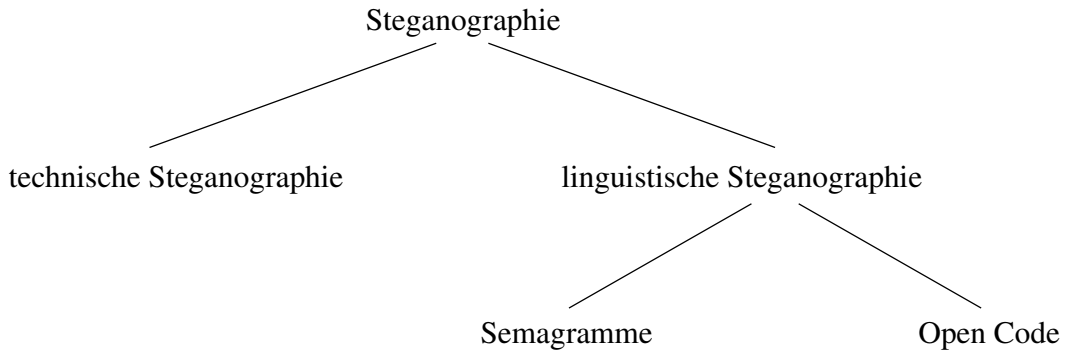


Abbildung 6.4: Einteilung der Steganographie

Methoden der technischen Steganographie sind zum Beispiel:

- Der Gebrauch von Geheimtinten wie z. B. Zitronensaft oder die Mischung von Zwiebelsaft und Milch. Beide Geheimtinten werden beim Erwärmen sichtbar.

- Das Verstecken der Nachricht in hohlen Schuhabsätzen, zwischen doppelten Böden, in ausgehöhlten Büchern, in Schirmgriffen usw.

Aufgrund der hohen Behaltensleistung originärer Erfahrungen sowie aus Gründen der Motivation, bietet es sich im Unterricht an, selbst eine Geheimtinte herzustellen und deren Tauglichkeit zu überprüfen.

Interesse wecken auch Ereignisse aus der Geschichte der technischen Steganographie. Im Unterricht könnten hierzu folgende Beispiele geschildert werden:

- Der Geschichtsschreiber Herodot[3)] berichtet in seinem Werk "Historien" von einem Schriftwechsel zwischen Histiaios und Aristagoras wie folgt: " Er [Histiaios] ließ also seinem getreuesten Sklaven den Kopf glatt rasieren, Zeichen darauf schreiben, das Haar wieder wachsen und schickte ihn dann nach Milet. Er gab ihm keinen anderen Auftrag als den, Aristagoras in Milet zu bitten, ihm das Haar scheren zu lassen und dann auf seinen Kopf zu sehen."[4)]

- In Herodots "Historien" befindet sich auch ein Bericht von Demaratos (ca. 510 bis ca. 491 v. Chr.), einem König in Sparta, der seine Herrschaft in Griechenland verloren hatte und freiwillig nach Susa in die Verbannung gegangen war. Dort erfuhr er, dass Xerxes – der König der Perser – einen Feldzug gegen Sparta beschlossen hatte. Demaratos wollte daraufhin die Spartaner warnen. "Weil er dies auf andere Weise nicht konnte – es bestand ja die Gefahr, dass es entdeckt würde –, ersann er folgende List: Er nahm eine zusammenlegbare Schreibtafel, schabte das Wachs davon ab und schrieb dann den Entschluss des Königs auf das Holz der Tafel. Danach überzog er die Buchstaben wieder mit Wachs, damit die leere Tafel bei den Straßenwächtern keinen Argwohn erweckte. Als die Tafel wirklich nach Sparta gelangte, verstanden die Lakedaimonier[5)] nicht, was die leere Tafel bedeuten sollte, bis schließlich Gorgo, die Tochter des Kleomenes und Gattin des Leonidas[6)], wie man erzählt, dahinter kam."[7)]

- Während des Zweiten Weltkrieges gelang es der deutschen Armee mithilfe der Mikrophotographie, eine ganze DIN A4 Seite als Mikropunkt – auch als Mikrodot bezeichnet – von der Größe eines Schreibmaschinenpunktes darzustellen. Dieser wurde häufig unter der Briefmarke oder in einer Postkarte versteckt, bei der man eine Ecke aufspaltete und nach dessen Hineinlegen wieder verklebte.

Die linguistische Steganographie umfasst zwei Methoden: Semagramme und Open Code Verfahren. Bei Semagrammen ist eine geheime Botschaft in Form von kleinen Details in einem harmlos erscheinenden Text oder Bild verborgen. Semagramme sind zum Beispiel:

[3)] Der als "Vater der Geschichtsschreibung" geltende griechische Historiker und Völkerkundler Herodot wurde zwischen 490 und 480 in Halikarnassos, einer Stadt im Südwesten Kleinasiens geboren. Um 465 wurde er vorübergehend aus seiner Heimat vertrieben und floh für 10 bis 15 Jahre nach Samos. Um 456 ging er nach Athen und einige Jahre später in die neu gegründete Stadt Thurioi in Unteritalien. Von dort unternahm er weite Reisen, u. a. nach Kyrene (im heutigen Libyen) und nach Athen. In Thurioi starb Herodot um 425.

[4)] [14], S. 679

[5)] Antike Bezeichnung für die Spartaner

[6)] Spartanischer König von 488 bis 480 v. Chr.

[7)] [14], S. 1051

- Die Verwendung unterschiedlicher Schriftarten, Absetzen bei Texten in Schreibschrift, geringfügiges Tieferstellen einzelner Buchstaben, das Kennzeichnen von Buchstaben durch Punkte oder Striche (evtl. auch mittels Geheimtinte) usw.
- Die Anordnung von langen und kurzen Grashalmen in Bildern, die der Adressat als Morsezeichen auffasst oder die Zeichnung eines herbstlichen Blattes, in dem der Adressat eine Landkarte mit feindlichen Stellungen erkennt.

Bei Open Code Verfahren wird eine scheinbar harmlose Nachricht offen mitgeteilt. Die eingebettete geheime Botschaft ist nur nach vorheriger Absprache mit dem Kommunikationspartner ersichtlich. Hierzu gehören:

- Maskierte Nachrichten, wie z. B. die Zeichen von Kartenschwindlern oder die Verwendung bestimmter Stichwörter, die ein besonderes Ereignis zum Ausdruck bringen.
- Verschleierte Nachrichten, bei denen bestimmte Buchstaben aus einem Text die geheime Botschaft ergeben (z. B. jeder x-te Buchstabe nach einem Satzzeichen) oder bei denen durch Auflegen einer Schablone bestimmte Wortteile ersichtlich werden, die die geheime Botschaft bilden.

Nach dieser Einführung in die Steganographie sollten die Schüler selbst Semagramme entwerfen. Die scheinbar unverfänglichen Texte können unter den Mitschülern ausgetauscht werden. Da die Schüler bereits für die Details der Semagramme sensibilisiert wurden, werden die meisten in der Lage sein, die verborgenen Nachrichten zu erkennen. Daran werden aber auch die Nachteile der Steganographie deutlich:

- Durch das Verbergen einer Nachricht in einem unverfänglichen Text, wirkt die Sprache desselben gestelzt.
- Für das geübte Auge sind Semagramme leicht zu erkennen.
- Bei genauer Prüfung einer scheinbar harmlosen Nachricht, wird auch eine Geheimtinte ersichtlich werden.
- Wird beim Gebrauch der technischen Steganographie die Nachricht durch gründliches Untersuchen entdeckt, liegt die Botschaft offen vor.

Zusammenfassend kann deshalb festgehalten werden, dass die Methoden der Steganographie allein nicht ausreichen, um Nachrichten vor unbefugten Dritten zu schützen. Vielmehr bedarf es einer Erhöhung der Sicherheit durch kryptographische Verfahren.

6.1.4 Zusammenfassung

In diesem Kapitel wird eine Einführung in einen Kryptologieunterricht durch Darlegung der Ziele der Kryptographie vorgeschlagen. Dadurch wird die Notwendigkeit der Datenverschlüsselung erkannt und durch geeignete Beispiele deren Bedeutung für die Praxis deutlich.

Anschließend werden Fachbegriffe im Bereich der Kryptologie eingeführt. Die Verschlüsselung wird dabei als Relation dargestellt, die einen Klartext in einen Geheimtext überführt. Dadurch

erkennen die Schüler, dass ein Klartextzeichen in mehrere Geheimtextzeichen überführt werden kann. Außerdem wird auf die Notwendigkeit der eindeutigen Entschlüsselung eines Geheimtextes eingegangen.

Um die Kryptographie deutlich als “offene” Geheimschrift zu kennzeichnen, wird eine kurze Einführung in den Bereich der Steganographie vorgeschlagen. Dadurch erlernen die Schüler sowohl grundlegende Techniken der Steganographie kennen, als auch typische Einsatzmöglichkeiten der versteckten Nachrichtenübermittlung. Aufgrund der Schwächen der Steganographie wird die Notwendigkeit der Verschlüsselung deutlich, womit ein Übergang zu symmetrischen Chiffrierverfahren gegeben ist.

6.2 Symmetrische Chiffrierverfahren

Bevor einzelne symmetrische Chiffrierverfahren behandelt werden, sollte die grundlegende Funktionsweise dieser kryptographischen Methoden bekannt sein. Im Unterricht eignet sich hierfür eine Darstellung wie z. B. Abbildung 6.5. Aus dieser gehen die charakteristischen Schritte symmetrischer Verschlüsselungsverfahren hervor:

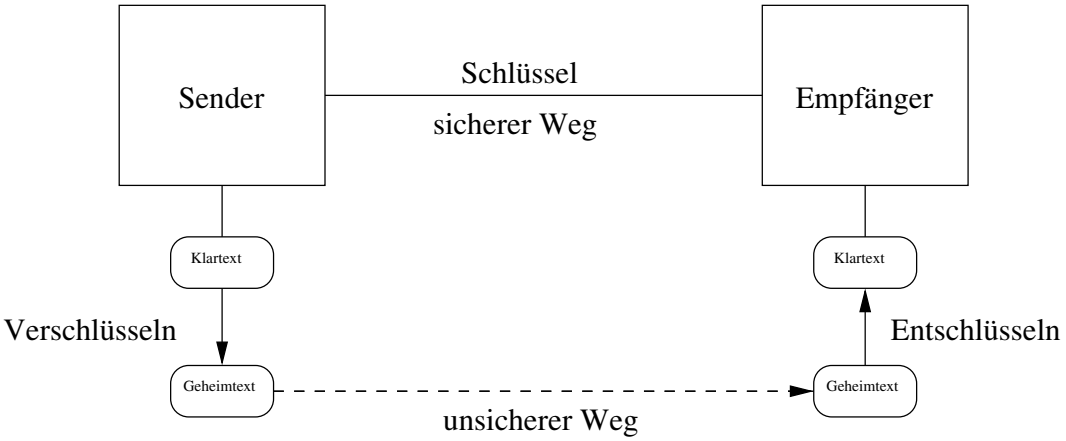


Abbildung 6.5: Verfahren der symmetrischen Verschlüsselung

1. Die beiden Kommunikationspartner müssen im Vorfeld einen Schlüssel auf einem sicheren Weg – wie z. B. bei einem persönlichen Treffen in abhörsicherer Umgebung – austauschen.
2. Der Sender einer Nachricht verschlüsselt nun den Klartext der Botschaft auf Grundlage des ausgetauschten Schlüssels und erhält den entsprechenden Geheimtext.
3. Der Geheimtext kann nun auf einem unsicheren Weg – wie z. B. per E-Mail – an den Empfänger geschickt werden.
4. Der Empfänger entschlüsselt den Geheimtext mithilfe des ausgetauschten Schlüssels und erhält auf diese Weise den Klartext.

6.2.1 Monoalphabetische Substitution

6.2.1.1 Caesar–Verschiebechiffre

Zur Einführung in die Technik der Verschlüsselung bietet sich die Caesar-Verschiebechiffre an. Diese Chiffre erfreut sich nicht nur eines ausgesprochen hohen Bekanntheitsgrades; sie weist auch einen historischen Bezug auf und ist zudem eine leicht verständliche Verschlüsselung.

Durch Erörterung der Schwächen der Caesar-Verschiebechiffre gelangt man unmittelbar zu den allgemeinen Formen der monographischen Substitution.

Intentionen

- Die Schüler sollen die Caesar–Verschiebechiffre mit unterschiedlichen Schlüsseln anwenden können.
- Die Schüler sollen die Schwächen der Caesar–Verschiebechiffre im Rahmen der Kryptanalyse erkennen.

Inhalte
Zur Einführung eignet sich ein (übersetzter) Bericht von Gaius Suetonius Tranquillus[8] über die Caesar–Chiffre. Neben dem motivierenden historischen Bezug wird die Verschlüsselungsmethode auch gut beschrieben:
"Es existieren auch Briefe von ihm [Caesar] an Cicero, desgleichen an seine Freunde über private Angelegenheiten, in denen er, wenn etwas geheim gehalten werden sollte, in einer Geheimschrift schrieb, d. h. er hat die Buchstaben so geordnet, dass kein Wort entziffert werden konnte: Wenn jemand gründlich nachforschen will, so möge er den vierten Buchstaben des Alphabets, d. h. D, für A setzen, und die übrigen entsprechend ordnen."[9]

Zur Veranschaulichung können zwei Alphabete auf Papierstreifen untereinandergelegt werden und gemäß der Vorgabe aus obigem Bericht angeordnet werden (vgl. Abbildung 6.6 und 6.7):

Klartextalphabet:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Geheimtextalphabet:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Abbildung 6.6: Das Geheimtextalphabet wird so weit verschoben, bis der Buchstabe D für den Klartextbuchstaben A steht.

Nach dieser Einführung sollten die Schüler in der Lage sein, selbstständig die Caesar–Verschlüsselung durchführen zu können. Dabei wird hier von einer mathematischen Darstellung

[8] Der römische Schriftsteller Gaius Suetonius Tranquillus ist zwischen 70 und 75 n. Chr. in Hippo Regius (im heutigen Algerien) geboren. Nicht zuletzt aufgrund des Ritterstandes seiner Familie gelangte Sueton an den Hof, wo er die Funktion von Redner und Anwalt ausführte. Bedeutenden politischen Einfluss erreichte er, als er das Amt des Kanzleichefs übernahm. Im Jahre 121 n. Chr. wurde Sueton mit einer Hofintrige in Verbindung gebracht und fiel dadurch bei Kaiser Hadrian in Ungnade, womit sich auch Informationen über sein weiteres Leben verlieren (vgl. [32], S. 181/182).

[9] [32], S. 77/79

Klartextalphabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Geheimtextalphabet:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Abbildung 6.7: Der "überhängende" Teil des Geheimtextalphabets wird abgeschnitten und hinter dem Buchstaben Z angefügt. Verschlüsselt wird jetzt, indem man die Buchstaben des Klartextes durch die darunter stehenden Buchstaben ersetzt.

der Caesar–Chiffre mithilfe der Modulo–Rechnung abgesehen und vielmehr die Motivation durch die Freude am Erstellen von Kryptogrammen gefördert. In einem weiteren Schritt ist der Verschiebe–Schlüssel – der bei Caesar 3 beträgt – zu variieren. Besondere Beachtung gilt dabei den beiden Schlüsselgrößen 13 und 25:

- Die Verschiebe–Verschlüsselung mit dem Schlüssel 13 ist als "ROT 13" bekannt geworden. Die Zuordnung der Klar- und Geheimtextbuchstaben ist symmetrisch (A $\rightarrow$ N und N $\rightarrow$ A). Folglich erhält man bei zweimaligem Anwenden dieser Verschlüsselung den Klartext.
- Bereits um 600 v. Chr. wurde in Palästina die Atbash–Verschlüsselung angewandt. Diese Verschlüsselung ist eine Verschiebe–Chiffre mit dem Schlüssel 25 und entspricht einer Umkehrung des Alphabets (A $\rightarrow$ Z und Z $\rightarrow$ A). Diese, ebenfalls symmetrische Geheimschrift, ist auch im Alten Testament aufzufinden. Zum Beispiel ist bei Jeremia 25,26 von "Scheschach" die Rede, was im Hebräischen einer Atbash–Chiffrierung von "Babel" entspricht.

Sofern die Lernenden über grundlegende Programmierkenntnisse verfügen, kann ein Programm zur Caesar–Chiffre auch ohne Einführung der Modulo-Rechnung mit Hilfe des ASCII-Codes erstellt werden. Im Anhang A (siehe Seite 154) befindet sich ein Beispiel eines solchen Programms mit der an bayerischen Realschulen eingeführten, objektorientierten Programmiersprache Visual Basic.

Kryptanalyse der Caesar–Chiffre
Neben dem Erstellen von Kryptogrammen, nehmen die Schüler auch Entschlüsselungen derselben (mit bekannten Schlüsseln) vor. Dabei erfolgt die Dechiffrierung ebenfalls mit Abbildung 6.7, indem die Geheimtextbuchstaben durch die darüber stehenden Buchstaben ersetzt werden.

Nun kann von der Lehrkraft ein verschlüsselter Text ohne Angabe des Schlüssels mit dem Auftrag zur Dechiffrierung ausgeteilt werden. Da noch keine Methoden der Kryptanalyse behandelt wurden, werden die Schüler durch Ausprobieren mehrerer Schlüssel versuchen, den Text zu entziffern. Es ist zu erwarten, dass bereits nach wenigen Minuten der erste Schüler mit dieser Methode erfolgreich ist.

Auf diese Weise sollen die Lernenden folgende Erkenntnisse erlangen:

- Durch systematisches Ausprobieren sämtlicher Schlüssel kann ein Kryptogramm entziffert werden.

- Bereits nach Ersetzen weniger Buchstaben zeigt sich, ob man mit dem gewählten Schlüssel Erfolg hat. D. h. ergeben sich bei den ersten Wörtern völlig sinnlose Buchstabenkombinationen, kann man die Dechiffrierung abbrechen.
- Die Verschiebechiffre ist aufgrund des kleinen Schlüsselraums von 26 Schlüsseln zu schwach und kann keine Sicherheit gewährleisten.

6.2.1.2 Monographische Substitution

Ausgehend von der Schwäche eines zu kleinen Schlüsselraums der Caesar–Verschiebechiffre, werden Überlegungen zur Erhöhung der Sicherheit angestellt. Dadurch kommt man auf die Forderung, die alphabetische Reihenfolge der Geheimtextbuchstaben nicht mehr bei zu behalten. Dies führt auf eine allgemeine Form der Verschlüsselung durch die monographische Substitution.

Beim Themenbereich der monographischen Substitution ist es aus Gründen der Übersichtlichkeit und zum besseren Verständnis wichtig, zwei Kategorien von Chiffren zu unterscheiden:

1. Ersetzung von Einzelzeichen durch einzelne Zeichen
2. Ersetzung von Einzelzeichen durch mehrere Zeichen

Die Substitution von Klartextzeichen durch mehrere Geheimtextzeichen wird im Unterricht auf der Grundlage der Schwächen der erstgenannten Chiffre hergeleitet.

Einzelzeichen werden durch Einzelzeichen ersetzt

Intentionen

- Die Schüler sollen die Ver- und Entschlüsselung bei monographischer Substitution durchführen können.
- Die Schüler sollen verschiedene Beispiele monographischer Chiffren kennen und anwenden können.
- Die Schüler sollen die Kryptanalyse mithilfe der Buchstabenhäufigkeit durchführen können.

Inhalte
Zur Einführung in den Themenbereich der monographischen Substitution genügt ein Beispiel, bei dem unter das Klartextalphabet ein permutiertes Alphabet (das Geheimtextalphabet) geschrieben wird. Verschlüsselt wird, indem jedes Klartextzeichen durch den darunter stehenden Buchstaben ersetzt wird. Die Dechiffrierung erfolgt durch die Ersetzung der Geheimtextzeichen durch die darüber stehenden Klartextbuchstaben.

Die Schüler erkennen, dass die beschriebene Zuordnung den Schlüssel dieser Chiffre darstellt. Da aus Sicherheitsgründen ein Schlüssel nicht schriftlich fixiert aufbewahrt werden darf, besteht ein Nachteil dieses Vorgehens darin, dass man sich die Zuordnung der einzelnen Zeichen nur

schwer merken kann. In der Vergangenheit hat sich deshalb die Erstellung des Geheimtextalphabets mithilfe eines Schlüsselwortes und eines Schlüsselbuchstabens als praktisch erwiesen:

- Sender und Empfänger einigen sich z. B. auf die monographische Substitution mit dem Schlüsselwort *Geheimnis* und dem Schlüsselbuchstaben *K*.
- Beim Schlüsselwort werden alle Buchstaben gestrichen, die zum wiederholten Mal auftreten. Man erhält damit aus obigem Schlüsselwort *Gehimns*.
- Unter das Klartextalphabet wird das Geheimtextalphabet geschrieben, indem beginnend beim Schlüsselbuchstaben *K*, das bearbeitete Schlüsselwort *Gehimns* geschrieben wird und die noch nicht verwendeten Buchstaben in alphabetischer Reihenfolge angehängt werden (vgl. Abbildung 6.8).

Klartextalphabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Geheimtextalphabet:	P	Q	R	T	U	V	W	X	Y	Z	G	E	H	I	M	N	S	A	B	C	D	F	J	K	L	O

Abbildung 6.8: Zuordnung der Geheimtextbuchstaben

Zu diesem Zeitpunkt ist darauf hinzuweisen, dass das Klar- und Geheimtextalphabet keineswegs über demselben Alphabet definiert sein müssen. Hierzu eignet sich die Darlegung von kryptographischen Beispielen aus der Geschichte der Kryptographie und der Literatur:

- Die Freimaurer – Mitglieder einer Gemeinschaft, die für Freiheit, Gleichheit, Brüderlichkeit, Toleranz und Humanität eintreten – entwickelten die Geheimschrift in Abbildung 6.9, die allerdings heute keine praktische Bedeutung mehr hat.

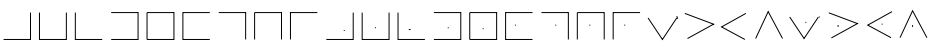
Klartextalphabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Geheimtextalphabet:																										

Abbildung 6.9: Die Freimaurerchiffre

- In der Erzählung “Der Goldkäfer” von Edgar Allan Poe ist ein durch monographische Substitution entwickeltes Kryptogramm zu entschlüsseln, das aus Zahlen, Satzzeichen und Sonderzeichen besteht.
- Ein sehr originelles Geheimtextalphabet stellt der Schriftsteller Arthur Conan Doyle in der Sherlock–Holmes–Geschichte “Die tanzenden Männchen” vor. Die Klartextbuchstaben werden hier durch Strichmännchen ersetzt.
- Dass auch Zahlen das Klartextalphabet darstellen können, zeigt die Kaufmanns–Chiffre, die zur Verschlüsselung des Verpackungsdatums bei Butter verwendet wurde. Hier werden die Zahlen 1;2;3;4;5;6;7;8;9;0 nacheinander mit den Buchstaben des Wortes MILCHPROBE verschlüsselt (z. B. bedeutet EMMI den 01.12.).

Kryptanalyse
Zur Einführung in die Kryptanalyse stellt es für die Schüler einen besonderen Anreiz dar, wenn

die Lehrkraft behauptet, jedes von den Schülern erstellte monographische Kryptogramm entschlüsseln zu können. Diese Behauptung ist im Unterricht zu belegen, wodurch die Lehrkraft die Häufigkeitsanalyse vorstellen kann. Alternativ kann auch ein Kryptogramm aus der Literatur (siehe oben) zur Entschlüsselung herangezogen werden.

Zunächst ist mit den Schülern zu erörtern, dass hier ein bloßes Ausprobieren aller Verschlüsselungsmöglichkeiten – im Gegensatz zur Caesar–Chiffre – nicht zum Erfolg führen kann. Über dem 26-elementigen Alphabet gibt es $26! \approx 4 \cdot 10^{26}$ verschiedene Möglichkeiten einer monographischen Substitution. Könnte jemand in einer Sekunde einen der möglichen Schlüssel testen, bräuchte er $26! \div (60 \cdot 60 \cdot 24 \cdot 365) \approx 1{,}28 \cdot 10^{19}$ Jahre, um sie alle zu überprüfen. Folglich muss es einen anderen Weg zur Kryptanalyse geben.

Wie Abbildung 6.10 zeigt, treten die einzelnen Buchstaben in der deutsche Sprache mit einer charakteristischen Häufigkeit auf. Der Buchstabe E ist mit 17,40 % am häufigsten vertreten, gefolgt von den Buchstaben N (9,78 %) und I (7,55 %).

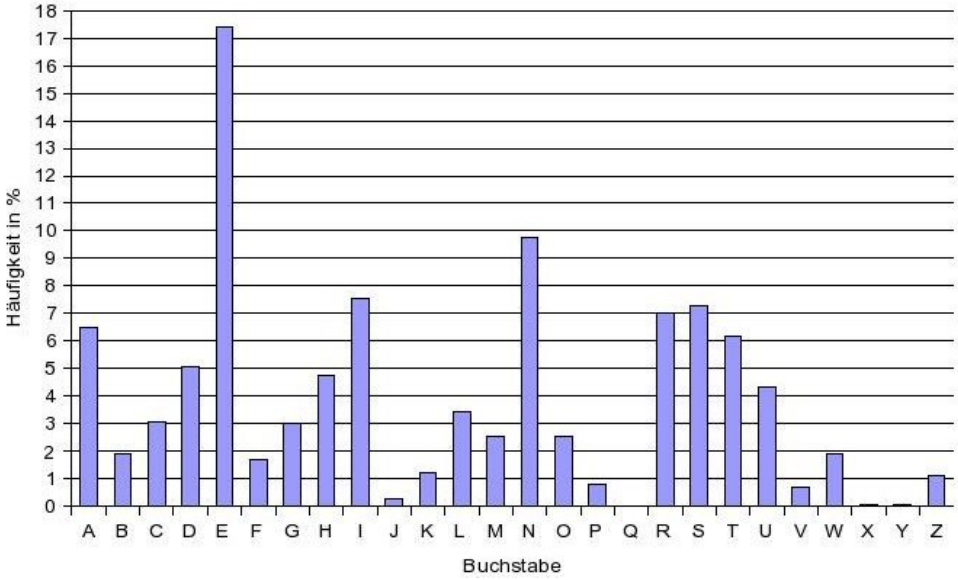


Abbildung 6.10: Buchstabenhäufigkeit in der deutschen Sprache

Zur Entschlüsselung des Kryptogramms

“ TYUBUI WUXUYHCUKC GPII HPI WPIO EUYRXC UICOYVVUAI”

kann man wie folgt vorgehen:

- Zuerst zählt man die Geheimtextziffern und bestimmt deren relative Häufigkeit. Auf diese Weise erhält man Anhaltspunkte auf die häufigsten drei Klartextbuchstaben. Im obigen Kryptogramm treten die Buchstaben U ($\approx$ 18,6 %), I ($\approx$ 16,3 %) und Y ($\approx$ 9,3 %) am häufigsten auf.
- Man kann davon ausgehen, dass die Geheimtextziffern U, I und Y den Klartextbuchstaben e, n und i entsprechen. Unterstützt wird diese Vermutung dadurch, dass das Buchstaben-

paar UY zweimal und YU einmal auftaucht. Das entsprechende Klartext–Bigramm ei und ie macht durchaus Sinn und tritt relativ oft auf.

- Man entschlüsselt die vermuteten Klartextäquivalente und erhält:

  TieBen WeXeiHCeKC GPnn HPn WPnO EeiRXC enCoiVVeAn

  Da dieses Kryptogramm sehr kurz ist, ist eine weitere Arbeit mit Hilfe der Buchstabenhäufigkeit zu unsicher.

- Deshalb beginnt man eine Tabelle anzufertigen, welche die Buchstabenzuordnung zur Ver- bzw. Entschlüsselung anzeigt (siehe Abbildung 6.11).

Klartextalphabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Geheimtextalphabet:					U				Y					I												

Abbildung 6.11: vorläufige Entschlüsselungstabelle

Ein Blick auf diese Tabelle legt die Vermutung nahe, dass der Geheimtext mit einem Schlüsselwort gebildet wurde, in dem die Buchstaben V, W, X nicht vorkommen; denn diese lassen sich zwischen den aufgedeckten Geheimtextbuchstaben U und Y alphabetisch hinzufügen.

Klartextalphabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Geheimtextalphabet:					U	V	W	X	Y					I												

Abbildung 6.12: vorläufige Entschlüsselungstabelle

- Eine weitere Entschlüsselung auf Grundlage obiger Vermutung liefert:

  TieBen geheiHCeKC GPnn HPn gPnO EeiRhC enCOiffeAn

- Nun kann man einzelne Wörter bereits erraten: der Wortteil “geheiH” lässt nur den Klartext “geheim” zu. Die Entschlüsselung von H als Klartextbuchstaben m liefert im Kryptogramm das 4. Wort: “mPn” kann nur “man” heißen. Damit ist der Geheimtextbuchstaben P als a entschlüsselt.

- Den Rest des Kryptogramms

  TieBen geheimCeKC Gann man ganO EeiRhC enCOiffeAn

  kann man nun durch Erraten und Ergänzen der Dechiffriertabelle als “Diesen Geheimtext kann man ganz leicht entziffern” aufdecken.

Wichtig ist, dass die Schüler selbst auch Entschlüsselungen durch die Häufigkeitsanalyse vornehmen. Dabei erlangen sie folgende Erkenntnisse:

- Je länger ein Kryptogramm, desto sicherer ist die Häufigkeitsanalyse.

- Die Häufigkeitsanalyse funktioniert nicht bei "Zungenbrechern" wie z. B. "Zehn zahme Ziegen ziehen zehn Zentner Zucker zum Zug" oder "Zwischen zwei Zwetschgenzweigen zwitschern zwei Schwalben".
- Das Erstellen eines Diagramms der Buchstabenhäufigkeit einer Caesar–chiffrierten Nachricht zeigt, dass das Häufigkeitsgebirge der deutschen Sprache (vgl. Abbildung 6.10) um die Schlüssellänge verschoben ist.

Zur Horizonterweiterung sollte Edgar Allan Poes Erzählung "Der Goldkäfer" gelesen werden. Die Entschlüsselung eines Kryptogramms wird hier nicht nur sehr anschaulich beschrieben (siehe Anhang B auf Seite 157). Diese Geschichte zeigt auch, dass Geheimtexte im Englischen mithilfe der Buchstabenhäufigkeit der englischen Sprache entsprechend gebrochen werden können. Außerdem bietet es sich im Unterricht an, die Geschichte nicht bis zur vollständigen Entschlüsselung des Kryptogramms zu lesen und einen Teil der Botschaft von den Schülern dechiffrieren zu lassen.

Einzelzeichen werden durch mehrere Zeichen ersetzt

Nachdem bei der Häufigkeitsanalyse monographischer Chiffren deutlich wurde, dass ein unbefugter Dechiffrierer anhand der Buchstabenhäufigkeit mit geringem Aufwand erfolgreich sein kann, wird jetzt versucht, den Anhaltspunkt der Kryptanalyse über die Buchstabenhäufigkeit zu umgehen. Ein Buchstabe wird folglich nicht mehr durch immer dasselbe Zeichen ersetzt, sondern durch mehrere Zeichen. Eine solche Verschlüsselung bezeichnet man auch als "homophone Chiffre".

Intentionen

- Die Schüler sollen homophone Chiffren entwickeln und anwenden können.
- Die Schüler sollen gezielt Blender und Spreizer zur Erhöhung der Sicherheit des Kryptogramms einsetzen können.
- Die Schüler sollen die Kryptanalyse durch Untersuchung von Buchstaben–Bigrammen kennen lernen.

Inhalte

Ausgangspunkt für die Entwicklung einer homophonen Chiffre ist wiederum die Buchstabenhäufigkeit einer natürlichen Sprache. Um eine gleichmäßige Verteilung von Zeichen im Kryptogramm zu erreichen, werden einem Klartextbuchstaben so viele Zeichen zugeordnet, wie dessen Häufigkeit entsprechen. So sind z. B. dem Buchstaben E mit einer Auftrittswahrscheinlichkeit von 17,40 % insgesamt 17 Geheimtextzeichen zuzuordnen, dem Buchstaben N mit einer relativen Häufigkeit von 9,78 % sind 10 Zeichen zuzuordnen usw.

Dabei ist zu beachten, dass ein Geheimtextzeichen nur jeweils genau einem Klartextbuchstaben zugeordnet werden darf, da sonst die Dechiffrierung nicht mehr eindeutig ist. Das Geheimtextalphabet muss folglich insgesamt mindestens 100 Zeichen umfassen. Für den Unterricht empfiehlt es sich daher, eine entsprechende monographische Chiffriertabelle mit zweistelligen

Zahlen aufzustellen. Bei der Verschlüsselung ist aus der Menge der einem Buchstaben zugeordneten Zeichen zufällig ein Geheimtextzeichen auszuwählen.

Neben der Entwicklung von homophonen Chiffren kann ein unbefugter Dechiffrierer auch durch den Einbau von Blendern und Spreizern getäuscht werden. Spreizer führen zu einer Erweiterung des Klartextalphabets um bestimmte Wörter bzw. Wortteile (Bigramme und Trigramme). Diesen Wörtern bzw. Wortteilen werden dann einzelne Geheimtextzeichen zugeordnet. Blender sind willkürlich dem Kryptogramm hinzugefügte Zeichen ohne Klartextäquivalente. Das bekannteste Beispiel einer monographischen Geheimschrift mit Blendern und Spreizern ist die Chiffre von Maria Stuart[10)], die im Unterricht – auch aufgrund der damit zusammenhängenden geschichtlichen Ereignisse – besprochen werden sollte (siehe Seite 159).

Kryptanalyse
Selbst bei der Nivellierung der Einzelzeichenhäufigkeit ist ein unbefugter Kryptoanalytiker nicht machtlos. Jede natürliche Sprache weist auch charakteristische Häufigkeitsverteilungen von Bigrammen (Buchstabenpaaren) auf.

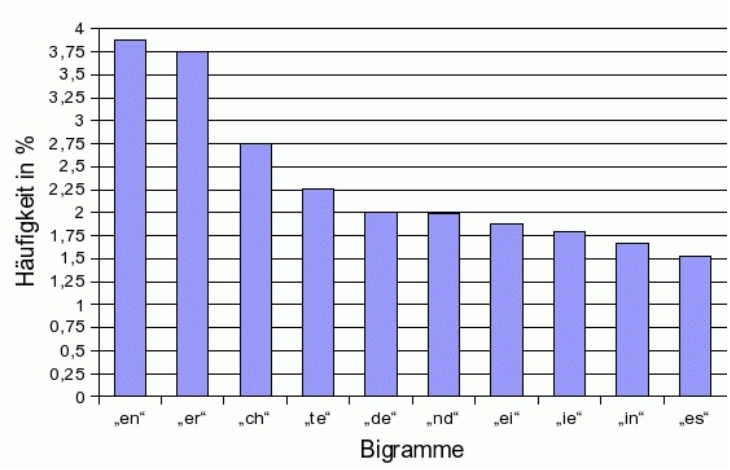


Abbildung 6.13: Häufigkeitsverteilung der Bigramme in der deutschen Sprache

Ist ein Kryptogramm lang genug, erhält der Dechiffrierer über die relative Häufigkeit entsprechender Zeichenpaare Hinweise auf die zugrunde liegenden Klartextbuchstaben. Hinzu kommt, dass bestimmte Buchstabenpaare wie z. B. “ei” auch in umgekehrter Reihenfolge d. h. als “ie” auftreten können – und das relativ gleich häufig. Dies ist bei Buchstabenpaaren wie z. B. ch oder ck nie der Fall.

In einem Unterricht in Kryptologie sollte auf solche kryptanalytischen Möglichkeiten hingewiesen und diese an einem Beispiel verdeutlicht werden. Allerdings empfiehlt es sich nicht, von Schülern diese Art der Kryptanalyse vornehmen zu lassen, da es sich um sehr langwierige Verfahren handelt.

[10)] Maria Stuart war in der Zeit vom 14.12.1542 bis 24.07.1567 Königin von Schottland. 1586 wurde sie – bereits nach 20 Jahre langer Haft – wegen Hochverrats angeklagt und am 08.02.1586 hingerichtet. Die Verurteilung erfolgte wesentlich auf der Grundlage von Briefen Maria Stuarts, die der britische Geheimdienst um Sir Francis Walsingham entschlüsseln konnte.

6.2.1.3 Polygraphische Substitution

Nachdem bisher die Ersetzung einzelner Klartextbuchstaben im Vordergrund stand, erfolgt durch Einführung der polygraphischen Substitution die Ersetzung mehrerer Buchstaben in einem Schritt. Dabei beschränkt sich der Lehrstoff in Kryptographie auf die Bigramm–Substitution. Die Trigramm–Substitutionen werden aufgrund der hohen Komplexität[11)] nicht behandelt.

Die älteste polygraphische Substitution wird in der 1563 erschienenen Abhandlung "De furtivis literarum notis" (Anmerkungen über versteckte Buchstaben) des Universalgelehrten Giovanni Battista della Porta beschrieben. Die von ihm stammende Bigramm–Substitution wurde durch eine Matrix festgelegt, die jedem Buchstabenpaar ein Geheimtextzeichen zuordnete.

Eine Bigramm–Chiffre mithilfe einer Matrix wie bei Porta, beansprucht bei einem 26-elementigen Alphabet insgesamt $26^2 = 676$ Geheimtextzeichen. Da folglich eine solche Zuordnung sehr aufwendig ist, soll im Unterricht die Bigramm–Substitution anhand der leichter durchführbaren Spezialfälle von Playfair oder Delastelle veranschaulicht werden.

Intentionen

- Die Schüler sollen die Bigramm–Substitution nach Playfair bzw. Delastelle durchführen können.
- Die Schüler sollen in der Lage sein, die Sicherheit des behandelten Verfahrens korrekt einzuschätzen.
- Die Schüler sollen die Festlegung eines Codes als eine polygraphische Chiffre kennen lernen.

Playfair–Verfahren

Die Playfair–Verschlüsselung wird im Folgenden in Form einer Arbeitsanweisung vorgestellt, anhand der die Schüler die Chiffrierung allein vornehmen können.

Die Nachricht: "Dieses Verfahren wurde von Wheatstone erfunden."[12)] soll mit dem Schlüsselwort "Playfair" durch das Playfair–Verfahren chiffriert werden. Beachte dabei folgende Vorgehensweise:

1. Beim Playfair–Verfahren wird die Nachricht zunächst unter Ausschluss von Leerzeichen und Satzzeichen in Buchstabenpaare eingeteilt. Der Buchstabe J wird in ein I umgewandelt, Buchstaben–Verdoppelungen werden durch den Einschub von X vermieden. Bei einem Text mit einer ungeraden Zeichenanzahl wird ein X angehängt.
2. Nun wird ein Geheimtextalphabet (ohne den Buchstaben J) erzeugt, indem ein Schlüsselwort ohne Buchstabenwiederholungen – beginnend links oben in der Ecke – zeilenweise

[11)] Bei einem 26-elementigen Alphabet sind 26^3 Fälle zu unterscheiden.

[12)] Das Playfair–Verschlüsselungsverfahren wurde 1854 vom britischen Physiker Charles Wheatstone erfunden. Dieser hat es seinem Freund Baron Lyon Playfair, einem britischen Chemiker und Politiker, vorgestellt. Playfair veröffentlichte dieses Chiffrierverfahren – unter Angabe des Erfinders Wheatstone – und schlug es zum Einsatz beim britischen Militär vor. Dort fand es auch bis zum Ersten Weltkrieg Anwendung.

in folgendes Quadrat (vgl. Abbildung 6.14) geschrieben wird. Der Rest des Quadrats wird mit den noch nicht verwendeten Buchstaben in alphabetischer Reihenfolge aufgefüllt.

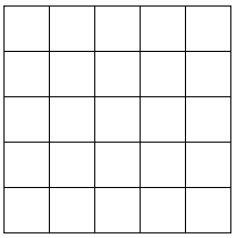


Abbildung 6.14: Quadrat zur Erzeugung des Geheimtextalphabets

3. Verschlüsselt wird, indem die Buchstabenpaare nach folgendem Verfahren ersetzt werden:
   - Stehen die Buchstaben in derselben Zeile, werden sie jeweils durch den rechten Nachbarn ersetzt. Steht ein Buchstabe am rechten Rand, setzt sich die Verschlüsselung in derselben Zeile am linken Rand fort.
   - Stehen die Buchstaben in derselben Spalte, werden sie jeweils durch den darunter stehenden Buchstaben ersetzt. Steht ein Buchstabe am unteren Rand, setzt sich die Verschlüsselung in derselben Spalte oben fort.
   - Stehen die Buchstaben in verschiedenen Zeilen und Spalten, denkt man sich diese als die Ecken eines Rechtecks. Als Geheimtextzeichen wählt man die Buchstaben der beiden anderen Eckpunkte. Dies bedeutet, dass ein Buchstabe durch den in derselben Zeile aber in der Spalte des jeweils anderen liegenden Buchstabens ersetzt wird.

Entschlüsselt wird, indem man Buchstaben in derselben Zeile bzw. Spalte jeweils durch den linken bzw. den darüber stehenden Buchstaben ersetzt. Stehen die Buchstaben in verschiedenen Zeilen und Spalten, geht man wie bei der Verschlüsselung vor.

Lösung des Arbeitsauftrags

1. Aus obiger Nachricht erhält man folgenden Text:

   DI ES ES VE RF AH RE NW UR DE VO NW HE AT ST ON EX ER FU ND EN

2. Das aus dem Schlüsselwort “Playfair” gewonnene Alphabet (ohne den Buchstaben J) ergibt die Matrix in Abbildung 6.15.

3. Die Verschlüsselung der Botschaft liefert folgendes Kryptogramm:

   IR KN KN UG LD BQ IG QU IV IM LV QU KG QF TN QO KU GI ZP IT NU

Kryptanalyse
Ein großer Nachteil der Playfair–Verschlüsselung ist, dass die Häufigkeit der Bigramme erhalten bleibt. Dadurch kann ein unbefugter Dechiffrierer – vorausgesetzt das Kryptogramm ist

P	L	A	Y	F
I	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

Abbildung 6.15: Aus dem Schlüsselwort “Playfair” gewonnenes Geheimtextalphabet

lang genug – über die Häufigkeitsanalyse der Bigramme Hinweise auf die zugehörigen Klartextbuchstabenpaare erhalten.

Ein weiterer Nachteil dieses Verfahrens besteht darin, dass die Ver- und Entschlüsselung von zwei Buchstaben in verschiedenen Zeilen und Spalten gleich ist. Hat nun ein unbefugter Dechiffrierer ein entsprechendes Buchstabenpaar entschlüsselt, erhält er damit auch die Klartexte zu drei weiteren Bigrammen. Wie im obigen Beispiel ersichtlich, wird ES durch KN chiffriert. Wird dieses Chiffrat aufgedeckt, erhält man damit auch, dass KN durch ES verschlüsselt wird, SE durch NK und NK durch SE.

Insofern ist dieses Verfahren heutzutage nicht mehr sicher und damit bedeutungslos geworden. Selbst eine abgeänderte Form des Playfair–Verfahrens mit zwei Matrizen, das im Zweiten Weltkrieg beim deutschen Militär unter dem Namen “Doppelkastenverfahren” oder “2–Tafel–Playfair” Einsatz fand, wurde von den Briten regelmäßig gebrochen [13)].

Delastelle–Verfahren

Auch das Verschlüsselungsverfahren nach Delastelle sollte in Form einer Arbeitsanweisung, anhand der die Schüler die Chiffrierung allein vornehmen können, behandelt werden.

Beispiel zur Beschreibung der Verschlüsselung:

1. Zunächst wird der Klartext ohne den Buchstaben W, sowie ohne Leerzeichen und Satzzeichen, in Buchstabenpaare eingeteilt.
2. Nun wird ein Geheimtextalphabet (ohne den Buchstaben W) erzeugt, indem ein Schlüsselwort ohne Buchstabenwiederholungen – beginnend links oben in der Ecke – zeilenweise in folgendes Quadrat (vgl. Abbildung 6.16) geschrieben wird. Der Rest des Quadrats wird mit den noch nicht verwendeten Buchstaben in alphabetischer Reihenfolge aufgefüllt.
3. Verschlüsselt wird, indem die Buchstabenpaare nach folgendem Verfahren ersetzt werden:
    - Bestimme zu jedem Zeichen eines Buchstabenpaars die Position im Quadrat durch Angabe der Zeilen- und Spaltenkoordinaten in der Form (Zeile,Spalte) und schreibe die Koordinaten beider Buchstaben hintereinander.

[13)] vgl. [2], S. 68

	1	2	3	4	5
1					
2					
3					
4					
5					

Abbildung 6.16: Quadrat zur Erzeugung des Geheimtextalphabets

- Vertausche die Zeilenkoordinate des 2. Zeichens mit der Spaltenkoordinate des 1. Zeichens (vgl. Abbildung 6.17).

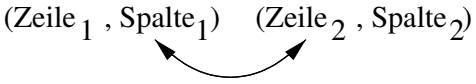


Abbildung 6.17: Vertauschen der Koordinatenangaben

- Bestimme zu den erhaltenen Koordinaten die Buchstaben des Quadrats und ersetze das Klartext–Buchstabenpaar durch diese.

Die Entschlüsselung erfolgt in derselben Weise wie die Chiffrierung.

Kryptanalyse
Wie auch beim Playfair–Verfahren bleiben bei der Verschlüsselung nach Delastelle die charakteristischen Häufigkeiten der Bigramme einer natürlichen Sprache erhalten, so dass ein unbefugter Dechiffrierer anhand eines genügend langen Kryptogramms Hinweise auf die zugrundeliegenden Klartext–Buchstabenpaare erhält.

Von Nachteil ist auch, dass Buchstabenpaare bei der Chiffrierung in sich selbst übergehen können. Dies geschieht immer dann, wenn das Zeichenpaar Koordinaten der Form (a,b)(b,c) aufweist.

Codes

Unter einem Code versteht man im weitesten Sinne eine Vorschrift um Daten einem Übertragungskanal anzupassen. So werden z. B. Schriftzeichen durch den ASCII–Code zur Datenverarbeitung am Computer in Bitfolgen oder durch den Morsecode in ein Ton- bzw. Funksignal umgewandelt.

Code im kryptologischen Sinne bedeutet, dass für Wörter, Satzteile oder ganzen Sätze Chiffrate festgelegt werden. Die Schüler sollen deshalb erkennen, dass polygraphische Chiffren nicht nur Buchstabenpaare verschlüsseln und weiter aufzufassen sind.

Eines der ersten Beispiele von Codes in diesem Sinne befindet sich in der Geheimschrift von Maria Stuart (vgl. Anhang C auf Seite 159). Häufig verwendete Begriffe werden durch einzel-

ne Zeichen ersetzt. Ist die Anzahl der codierten Wörter bzw. Sätze größer, sind Listen[14] mit Klartexten und zugehörigen Codes anzufertigen. Später wurden solche Listen zu Büchern, den Codebüchern, zusammengefasst.

Im Unterricht eignet es sich, einige Beispiele aus Codebüchern zu zeigen und deren Vor- und Nachteile zu erarbeiten. Zum Beispiel wurde von den Deutschen während des Ersten Weltkrieges das "Signalbuch der kaiserlichen Marine" (SKM) verwendet. Hier bedeutete z. B. 53439 Bohle, 53440 Bohne, 53441 bohren, 53442 Bohrer, 53443 Boje, Bojen usw. Bei einem alphabetisch und numerisch geordneten Code – als einteiliger Code bezeichnet – ist sowohl zur Verals auch zur Entschlüsselung nur ein Codebuch notwendig. Ein großer Nachteil ist allerdings, dass ein unbefugter Dechiffrierer bei Kenntnis einzelner Codes ein Wort erraten kann, da es in alphabetischer Reihenfolge angeordnet ist.

Aufgrund dieses Nachteils einteiliger Codebücher wurden später zweiteilige Codebücher entwickelt, bei denen die Codes keine Struktur mehr aufwiesen. Allerdings mussten nun zwei Codebücher verwendet werden: zur Verschlüsselung nach Klartexten alphabetisch geordnet, zur Entschlüsselung nach Codegruppen geordnet. Doch auch diese beinhalten – wie alle Codebücher – eine große Gefahr: Bei Verlust bzw. Diebstahl verliert ein Kryptogramm jegliche Sicherheit.

Bei diesem Thema eignet sich auch der Einsatz von Berichten über den Verlust des Signalbuchs der kaiserlichen Marine durch die Einnahme des deutschen Kreuzers "Magdeburg" sowie über die Entschlüsselung des "Zimmermann–Telegramms", was letztendlich den Kriegseintritt der USA in den Ersten Weltkrieg entschied[15].

6.2.2 Transposition

Die bisher behandelten Chiffrierverfahren haben gemeinsam, dass Klartextzeichen durch andere Zeichen ersetzt wurden. Bei Transpositionen wird ein Klartextbuchstabe nicht durch andere Zeichen ersetzt, sondern er ändert seine Position im Text. Die Verschlüsselung stellt also eine Permutation der Klartextzeichen dar.

Intentionen

- Die Schüler sind in der Lage, die kryptographischen Verfahren der Transposition von denen der Substitution zu unterscheiden.
- Die Schüler können die Spalten- bzw. Zeilen–Transposition mithilfe einer Matrix durchführen.
- Die Schüler können die Transposition mit einem geeigneten Raster anwenden.
- Die Schüler können die Sicherheit dieser Verfahren richtig einschätzen.

[14] Eine solche Liste wird als Nomenklator bezeichnet.
[15] Beide Ereignisse sind in [20] unter "Codebücher im Ersten Weltkrieg" sehr ausführlich beschrieben.

Inhalte
Als Einführung in das Thema der Transposition eignet sich die Vorführung der Chiffrierung mit der Skytale, die die Spartaner bereits im 5. Jahrhundert v. Chr. angewandt haben. Deren Funktionsweise wird vom griechischen Historiker Plutarch[16] ausführlich beschrieben:
"Mit der Skytale hat es folgende Bewandtnis. Wenn die Euphoren[17] einen General oder Admiral ausschickten, ließen sie zwei runde Stäbe von gleicher Dicke und Länge anfertigen, so dass sie an den Enden genau zusammenpassten; den einen davon behielten sie selbst, den anderen gaben sie dem ausgesandten Befehlshaber mit. Diese Stäbe nannten sie Skytalen. Wenn sie ihm nun etwas Geheimes und Wichtiges mitteilen wollten, wanden sie ein schmales und langes Papier in Form eines Riemens um die zurückbehaltene Skytale, so dass nicht der geringste Zwischenraum blieb, sondern dessen ganze Oberfläche ringsherum mit dem Papier bedeckt wurde. Dann schrieben sie, was sie wollten, auf das Papier, wie es um den Stab gewunden war, nahmen das beschriebene ab und schickten es ohne den Stab an den Feldherrn. Dieser konnte nun den erhaltenen Brief, der ohne Zusammenhang und auseindergerissen war, nicht anders lesen, als wenn er den Papierstreifen um seine Skytale herumwand, wodurch die Windung wieder in die gehörige Ordnung kam, das zweite sich an das erste anschloss und das Auge nun um den Stab herum den Zusammenhang finden konnte. Der Brief hieß ebenso wie der Stab Skytale, wie man auch sonst das Gemessene nach dem Maße zu nennen pflegt."[18]

Im Unterricht sollte diese Beschreibung der Verschlüsselung mithilfe einer Skytale an einem nachgebauten Beispiel veranschaulicht werden. Zum Beispiel erhält man mit einer Skytale von 3,8 cm Durchmesser und einem Papierstreifen von 4,5 cm Breite und 75 cm Länge für die Botschaft

"Mein geheimnisvoller Durchmesser"

das Kryptogramm

"Mhsrm eevDe iious nmlrs gnlce eiehr".

Durch dieses Beispiel wird bei den Schülern die Neugier für Transpositionen geweckt. Sie erkennen, dass ohne Substitution von Buchstaben ein Kryptogramm erstellt wurde, das nur mithilfe eines Stabes von genau demselben Durchmesser wie der Skytale entschlüsselt werden kann. Außerdem wird deutlich, dass bei Transpositionen eine Kryptanalyse mithilfe der Buchstabenhäufigkeit nicht möglich ist. Die Häufigkeitsanalyse kann lediglich den Hinweis liefern, dass die Verschlüsselung durch Transposition erfolgt ist, da jeder Buchstabe seine charakteristische Auftrittswahrscheinlichkeit im Kryptogramm beibehält.

Spalten- und Zeilen–Transposition
Im Unterricht kann die Spalten–Transposition durch eine Analyse des obigen Beispiels eingeführt werden: Auf der Skytale (siehe oben) werden immer sechs Buchstaben in einer Reihe

[16] Plutarch wurde um 50 n. Chr. in Chaironeia als Sohn einer angesehenen Familie geboren. Während seines Studiums der Philosophie schloss er sich der platonischen Akademie an. Trotz ausgedehnter Reisen nach Asien, Alexandria und Italien kehrte er immer wieder in seine Geburtsstadt zurück. Plutarch starb 120 n. Chr. in Delphi, wo er das Amt des Apollonpriesters inne hatte.
[17] Leiter der Politik in Sparta. Insgesamt fünf Euphoren wurden für ein Jahr gewählt und hatten beachtliche politische Macht, u. a. ein Vetorecht gegen die Könige.
[18] [27], S. 170

aufgeschrieben bevor mit einer 1/5–Drehung eine neue Zeile begonnen wird. Diese Darstellung wird nun mit Hilfe einer Matrix, bestehend aus 6 Spalten und 5 Zeilen, nachgeahmt. Hierzu wird der Klartext zeilenweise in die 6x5 Matrix eingeschrieben (vgl. Abbildung 6.18).

M	E	I	N	G	E
H	E	I	M	N	I
S	V	O	L	L	E
R	D	U	R	C	H
M	E	S	S	E	R

Abbildung 6.18: Die Spalten–Transposition

Ein Vergleich des obigen Kryptogramms mit dieser Matrix zeigt, dass der Geheimtext

”MHSRM EEVDE IIOUS NMLRS GNLCE EIEHR”.

durch spaltenweises Auslesen der Nachricht aus der Matrix entsteht.

Dasselbe Kryptogramm erhält man auch, wenn man den Klartext spaltenweise in eine Matrix mit 5 Spalten und 6 Zeilen einschreibt und anschließend zeilenweise ausliest:

M	H	S	R	M
E	E	V	D	E
I	I	O	U	S
N	M	L	R	S
G	N	L	C	E
E	I	E	H	R

Abbildung 6.19: Die Zeilen–Transposition

Dieser Transposition widmet der Schriftsteller Julius Verne in seinem Roman “Reise zum Mittelpunkt der Erde” ein Kapitel. In diesem geht es um die Entzifferung eines alten Dokuments, das den Weg ins Erdinnere weist. Im Unterricht bietet sich der Einsatz dieser Literatur für den Übergang zur Kryptanalyse an (siehe Anhang D auf Seite 160).

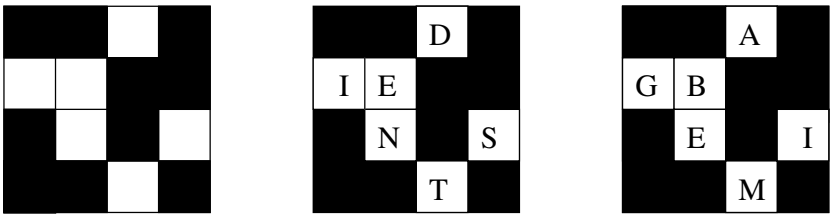
Aus diesem Textausschnitt geht eindeutig hervor, wie ein Kryptogramm aus einer Spalten- bzw. Zeilen–Transposition gebrochen werden kann. Die Schüler erkennen, dass durch eine Aneinanderreihung des ersten, zweiten, dritten usw. Buchstabens aus jedem Buchstaben–Block der Klartext entsteht. Insofern bietet die Spalten- bzw. Zeilen–Transposition keine hohe Sicherheit. Im Unterricht sollten deshalb Möglichkeiten entwickelt werden, mit denen die Sicherheit einer solchen Chiffre erhöht werden kann:

- Nach dem Einschreiben des Klartextes in eine Matrix führt eine Vertauschung von Zeilen oder Spalten zu einer besseren Durchmischung der Buchstaben.

- Nach dem Auslesen des Kryptogramms kann dieses ohne Lücken d. h. ohne Buchstabenblöcke oder in umgekehrter Reihenfolge aufgeschrieben werden.

Raster
Eine einfach zu bedienende Transposition besteht in der Verwendung eines Rasters. Hierbei handelt es sich um eine (meist quadratische) Schablone, bei der in die vorhandenen Lücken der Klartext buchstabenweise eingeschrieben wird. Anschließend werden die von der Schablone verdeckten Felder mit Buchstaben aufgefüllt. Das Kryptogramm kann jetzt nur nach Auflegen derselben Schablone entziffert werden (vgl. Abbildung 6.20).

Verschlüsselung von "Dienstag beim ..." mithilfe des folgenden Rasters



ergibt z. B. das Chiffrat:

A	B	D	O		G	H	A	L
I	E	P	R		G	B	Ö	I
E	N	W	S		C	E	Z	I
A	S	T	F		U	R	M	K

Abbildung 6.20: Transposition mithilfe eines Rasters

Die Sicherheit der Chiffrierung mit einem Raster kann erhöht werden, wenn beim Auffüllen der verdeckten Felder ein sinnvoller Text eingesetzt wird. Daneben sollten mehrere verschiedene Raster (Schablonen) Anwendung finden.

Der Schriftsteller Julius Verne hat sich auch in seinem Roman “Mathias Sandorf” mit der kryptographischen Methode des Rasters befasst. Da hier dem Leser sowohl die Vorteile als auch die Gefahr der Raster–Transposition vor Augen geführt werden, sollten entsprechende Auszüge aus diesem Roman im Unterricht eingesetzt werden (siehe Anhang E auf Seite 161). Daneben wird die Funktionsweise eines Drehrasters sehr gut beschrieben. Bei diesem entsteht das Kryptogramm, indem dasselbe Raster auf derselben Stelle, d. h. auf demselben Buchstabenquadrat viermal durch Drehung angewandt wird. Erst danach wird ein neues Buchstabenquadrat begonnen.

6.2.3 Polyalphabetische Substitution

Die bisher behandelten Verschlüsselungen werden als monoalphabetische Chiffrierverfahren bezeichnet. Sie sind dadurch gekennzeichnet, dass ein Chiffrierschritt wiederholt angewandt wird. Bei polyalphabetischen Verfahren findet dagegen ein Wechsel der Chiffrierschritte statt.

Im Unterricht sollte bei diesem Thema nicht nur die am weitesten verbreitete polyalphabetische Substitution nach Vigenère behandelt werden. An den leichter zu verstehenden frühen Verfahren wird für Schüler nicht nur der Unterschied zu monoalphabetischen Chiffren verständlich. Die Vorführung derselben bereitet auch auf die komplexere Vigenère–Verschlüsselung vor.

Intentionen

- Die Schüler sollen in der Lage sein, monoalphabetische und polyalphabetische Chiffrierverfahren zu unterscheiden.
- Die Schüler sollen die Entwicklung polyalphabetischer Verschlüsselungsverfahren in groben Zügen beschreiben können.
- Die Schüler sollen in der Lage sein, die Vigenère–Verschlüsselung durchführen zu können.
- Die Schüler sollen die Kryptanalyse Vigenère–chiffrierter Texte erfolgreich durchführen können.
- Die Schüler sollen Methoden zur Erhöhung der Sicherheit der Vigenère–Verschlüsselung herleiten können.

Diese Lernziele erfordern die unterrichtliche Behandlung der folgenden Themenbereiche.

6.2.3.1 Frühe Verfahren

Als “Vater der modernen Kryptologie” gilt der italienische Schriftsteller, Mathematiker, Architekt und Kryptologe Leon Battista Alberti. Aufbauend auf den Schwächen monoalphabetischer Chiffren schlug er 1466 in seinem Werk “De cifris” vor, das Geheimtextalphabet nach jeweils drei oder vier Wörtern zu wechseln.

Zum Beispiel würden die ersten drei Wörter einer Nachricht mit dem Geheimtextalphabet 1, die nächsten drei mit dem Geheimtextalphabet 2 substituiert werden, bevor wieder zum Geheimtextalphabet 1 gewechselt wird usw. (vgl. Abbildung 6.21).

Von Alberti stammt auch die Entwicklung einer Chiffrierscheibe zur Vereinfachung der Verschlüsselung. Eine Chiffrierscheibe besteht aus zwei unterschiedlich großen Scheiben, an deren Rändern Alphabete markiert sind. Am Rand der größeren Scheibe befindet sich dabei das Klartextalphabet, am Rand der kleineren Scheibe das Geheimtextalphabet. Die kleinere Scheibe wird in der Mitte der größeren Scheibe so befestigt, dass sie gedreht werden kann. Wird während der Verschlüsselung die Stellung der Scheiben nicht verändert, erhält man eine mono-

Klartextalphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Geheimtextalphabet 1	P	A	G	M	U	Z	I	B	H	N	V	S	C	J	O	W	T	D	K	Q	X	E	F	L	R	Y
Geheimtextalphabet 2	H	E	N	F	O	S	X	U	T	B	G	P	Y	M	A	D	J	Q	V	Z	L	I	C	K	W	R

Abbildung 6.21: Veranschaulichung einer polyalphabetische Substitution mit zwei Geheimtextalphabeten

alphabetische Substitution; bei einer Veränderung der Scheibenstellung, eine polyalphabetische Substitution.

Im Unterricht sollte eine polyalphabetische Substitution sowohl mithilfe einer Auflistung der Geheimtextalphabete (vgl. Abbildung 6.21), als auch mithilfe einer Chiffrierscheibe veranschaulicht werden. Außerdem sollte – sofern noch nicht zu einem früheren Zeitpunkt geschehen – eine Chiffrierscheibe aus Pappe gebastelt werden. Denn an dieser wird das Rotationsprinzip der später zu behandelnden Chiffriermaschinen besonders deutlich.

Aufbauend auf Albertis Erkenntnissen schlug 1508 der Abt im Kloster Sponheim (in Rheinland–Pfalz) Johannes Trithemius vor, bereits nach jedem Buchstaben das Geheimtextalphabet zu wechseln. Von ihm stammt auch die erste Chiffriertafel[19)], in der alle 25 möglichen Verschiebealphabete untereinander der Reihe nach aufgelistet sind (vgl. Abbildung 6.22). Die Verschlüsselung nach Trithemius erfolgt, indem nach jedem Buchstaben zum nächsten Verschiebealphabet übergegangen wird. Insofern entspricht diese Chiffre einer Vigenère–Verschlüsselung mit dem Schlüssel ABC...XYZ.

Zur Vorbereitung auf die Verschlüsselung nach Vigenère sollte im Unterricht sowohl die Chiffriertafel vorgestellt, als auch die Verschlüsselung nach Trithemius durchgeführt werden. Die Schwachstelle dieser Chiffre zeigt sich bei alphabetisch in umgekehrter Reihenfolge auftretenden Buchstaben (wie z. B. “fed”): diese werden jeweils durch denselben Buchstaben verschlüsselt.

Im Jahr 1553 schlug Giovanni Battista Belaso die Verwendung eines Schlüsselwortes für die Auswahl der Geheimtextalphabete vor. Jetzt waren es mehrere Kryptologen, welche die folgende Vigenère–Verschlüsselung erkannten: der italienische Arzt und Universalgelehrte Battista Della Porta (1535 - 1615), der italienische Arzt, Mathematiker und Philosoph Gironimo Cardano (1501 - 1576) und der französische Diplomat Blaise de Vigenère (1523 - 1596). Aufgrund ihrer Beiträge zur Kryptographie sollten alle drei Personen im Unterricht Beachtung finden.

6.2.3.2 Vigenère–Verschlüsselung

Das heute am bekanntesten polyalphabetische Chiffrierverfahren besteht aus einem Schlüsselwort und dem Vigenère–Quadrat (vgl. Abbildung 6.22).

[19)] Trithemius bezeichnete seine Chiffriertafel mit “tabula recta”. Heute ist sie unter dem Begriff “Vigenère–Tafel” bzw. “Vigenère–Quadrat” bekannt.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Abbildung 6.22: ‘tabula recta‘ des Trithemius bzw. Vigenère–Quadrat

Die Verschlüsselung nach Vigenère unterscheidet sich von der nach Trithemius dadurch, dass nicht alle Geheimtextalphabete des Vigenère–Quadrats zur Verschlüsselung herangezogen werden, sondern nur ein Teil davon. Zur Auswahl der Verschiebealphabete dient das Schlüsselwort. Hierzu wird das Schlüsselwort (z. B. Maus) zeichenweise unter den Klartext (“Angriff erfolgt morgen um...”) geschrieben und zwar so oft, bis die Länge der Nachricht erreicht ist (vgl. Abbildung 6.23).

A	n	g	r	i	f	f		e	r	f	o	l	g	t		m	o	r	g	e	n		u	m	...
M	A	U	S	M	A	U		S	M	A	U	S	M	A		U	S	M	A	U	S		M	A	...

Abbildung 6.23: Das Schlüsselwort wird zeichenweise unter den Klartext geschrieben.

Die Schlüsselbuchstaben unter den Klartextzeichen geben nun an, mit welchem Geheimtextalphabet der jeweilige Buchstabe chiffriert wird: man wählt das Verschiebealphabet, bei dem der Schlüsselbuchstabe in der ersten Spalte des Vigenère–Quadrates steht.

Für obige Nachricht erhält man so als Geheimtext “MNAJUFZ WDFIDST GGDGYF GM ...”.

Zur Einführung empfiehlt sich im Unterricht, zwei rechteckige Schablonen (z. B. aus Pappe) zu verwenden, die einen sichtbaren Bereich von der Länge des Vigenère–Quadrats und der Breite eines Buchstabens haben. Die erste Schablone wird waagrecht auf dem Vigenère–Quadrat verschoben, bis die Spalte mit dem Klartextbuchstaben in der ersten Zeile erscheint. Die zweite Schablone wird senkrecht auf dem Vigenère–Quadrat verschoben, bis der entsprechende Schlüsselbuchstaben in der ersten Spalte des Quadrats auftaucht. Das Geheimtextzeichen befindet sich im Schnittpunkt beider Schablonen (vgl. Abbildung 6.24).

Eine weitere Möglichkeit besteht darin, eine Chiffrierscheibe zur Verschlüsselung zu verwenden. Wie bei der Caesar–Chiffre muss hierbei das Geheimtextalphabet mit dem Klartextalphabet übereinstimmen. Zur Verschlüsselung wird die innere Scheibe so weit gedreht, bis der entsprechende Schlüsselbuchstabe unter dem “A” des Klartextalphabets auf der größeren Scheibe steht.

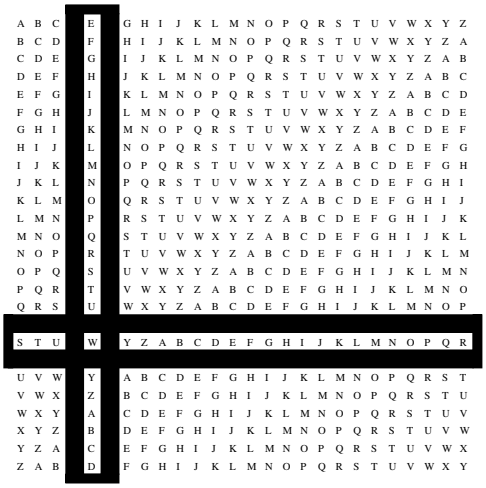


Abbildung 6.24: Der Buchstabe “e” des Wortes “erfolgt” wird durch “W” ersetzt.

Bei dieser Stellung erfolgt die Verschlüsselung des Klartextzeichens. Anschließend wird die innere Scheibe zur entsprechenden Stellung des nächsten Schlüsselbuchstabens gedreht usw.

Die Vigenère–Verschlüsselung galt über 200 Jahre als sicheres kryptographisches Verfahren, bis der preußische Infanteriemajor Friedrich Wilhelm Kasiski in seinem Werk “Die Geheimschriften und die Dechiffrierkunst” 1863 eine Anleitung zur Kryptanalyse Vigenère–chiffrierter Texte veröffentlichte.

6.2.3.3 Kryptanalyse

Bisher konnte aufgrund der Buchstabenhäufigkeit eines Kryptogramms auf das verwendete Verschlüsselungsverfahren geschlossen werden: Bei Transpositionen entspricht die Buchstabenhäufigkeit der Geheimtextzeichen der charakteristischen Häufigkeit der verwendeten Sprache. Bei einfachen monographischen Chiffren erhält man ein entsprechend abweichendes Häufigkeitsgebirge der Buchstaben, während bei homophonen Chiffren und polygraphischer Substitution die großen Unterschiede im Häufigkeitsgebirge reduziert sind.

Unter Einbeziehung polyalphabetischer Substitution lässt sich das verwendete Verschlüsselungsverfahren nicht mehr so eindeutig nachweisen. Deshalb sollte an dieser Stelle das Prinzip von Kerckhoffs[20)] eingeführt werden.

Prinzip von Kerckhoffs:

> Die Sicherheit eines kryptographischen Systems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich einzig und allein auf die Geheimhaltung des Schlüssels.

[20)] Der niederländische Linguist und Kryptologe Auguste Kerckhoffs stellte 1883 in seinem Werk “La Cryptographie militaire” Anforderungen an kryptographische Verfahren auf. Das nach ihm benannte Kerckhoffs–Prinzip gilt heute als Maßstab für moderne Verschlüsselungsverfahren.

Zur Beurteilung der Sicherheit kryptographischer Verfahren geht man also grundsätzlich davon aus, das Verschlüsselungsverfahren zu kennen. Folglich wird die Sicherheit der Vigenère–Chiffre danach beurteilt, wie leicht sie bei Kenntnis des Algorithmus zu brechen ist.

Im Unterricht empfiehlt sich, die Kryptanalyse der Vigenère–Verschlüsselung in drei Schritten vorzunehmen:

1. Scheitern der Häufigkeitsanalyse und von Brute–Force–Angriffen;
2. Kryptanalyse bei Kenntnis der Länge des Schlüsselwortes;
3. Test zum Auffinden der Länge des Schlüsselwortes.

Zum Auffinden der Länge eines Schlüsselwortes Vigenère–chiffrierter Texte sind zwei Methoden bekannt: Der Kasiski–Test von Friedrich Wilhelm Kasiski und der Kappa–Test von William Frederick Friedman[21)].

In dieser Arbeit ist vorgesehen, im Unterricht nur den Kasiski–Test durchzuführen. Zwar sind beide Tests zur Bestimmung der Schlüsselwortlänge gleich erfolgreich; der Kasiski–Test besitzt allerdings gegenüber dem Kappa–Test (auch Friedman–Test genannt) folgende Vorteile:

- Der Kasiski–Test kann anschaulich direkt am Kryptogramm erläutert werden, indem wiederholende Buchstabenkombinationen untersucht werden.
- Das mathematische Vorwissen beschränkt sich beim Kasiski–Test auf die Primfaktorzerlegung von natürlichen Zahlen.
- Beim Kappa–Test werden durch Einführung neuer Größen wie z. B. “Koinzidenzindex” und durch die Benutzung der Summenformel größere mathematische Leistungen beansprucht.
- Der Kappa–Test ist eine statistische Methode ohne Bezug zum Schulstoff aus anderen Fächern.
- Der Friedman–Test ist durch Berechnungen und Erstellung von Diagrammen ein sehr langwieriges Verfahren.

1. Häufigkeitsanalyse und Brute–Force–Angriffe
Im Unterricht sollten Überlegungen zur Kryptanalyse an einem Beispiel veranschaulicht werden. In dieser Arbeit wird das nachfolgende Kryptogramm als Beispiel herangezogen. Dabei wurde der Klartext ohne Satzzeichen und Leerzeichen nach Vigenère verschlüsselt. Zur besseren Übersicht ist das Kryptogramm in Buchstabenblöcke unterteilt.

Zur Kryptanalyse sollte im Unterricht zunächst die bisher bewährte Methode der Häufigkeitsanalyse untersucht werden. Hierzu werden die relativen Häufigkeiten der Geheimtextbuchsta-

[21)] William F. Friedman wurde 1891 in Moldawien (damals Russland) geboren, kurz bevor die Familie nach Amerika auswanderte. Dort wurde er Kryptologe und gründete noch vor Ausbruch des 2. Weltkrieges eine Dechiffrierabteilung beim US-Militär, die sich mit der Entschlüsselung feindlicher Nachrichten befasste. Seine Methode zur Analyse der Schlüsselwortlänge Vigenère–chiffrierter Texte veröffentlichte er 1920. William F. Friedman starb am 12.11.1969.

W O L A V O I A I E K A B V V O N I G Y X A L H Z F K L C G

U O F S X J E X M V M E B V V S V I R U F N A I Y F I G W T

I R C J K F N O R U J H L I I V N V I W V G N I E F N N D Z

G F Y V L O G Y M E S E W L K J M P I I C O L K V O E H F C

V E B I E E E L D N F I A F C V E B I E E W Y M C W O H E C

U E L W Y F R C L I F P L S W F S M M F O E F P V O V Y V K

S E N I I H U N I I O A Y L I F N X

Abbildung 6.25: Zu entschlüsselndes Kryptogramm

ben bestimmt. Im vorliegenden Kryptogramm ist der häufigste Buchstabe “J” mit 11,1 %, gefolgt von den Buchstaben “E” mit 8,6 % und “F” mit 8,1 %.

Bereits anhand dieser Größen ist zu erkennen, dass es sich bei vorliegendem Kryptogramm nicht um eine einfache monoalphabetische Verschlüsselung handeln kann. Denn dann wäre das dem “E” entsprechende Geheimtextzeichen mit einer Häufigkeit von ca. 17,4 % vertreten. Die Einzelzeichenhäufigkeiten werden also bei der Vigenère–Verschlüsselung nivelliert. Noch stärker tritt dies zu Tage, wenn ein langes Schlüsselwort verwendet wird. Dann bewegen sich die relativen Häufigkeiten der Geheimtextzeichen zwischen 8 und 1 Prozent. Insgesamt ist folglich festzustellen, dass die Häufigkeitsanalyse bei Vigenère–verschlüsselten Kryptogrammen keinen Beitrag zur Kryptanalyse leisten kann.

Eine andere Möglichkeit das Kryptogramm zu entschlüsseln, besteht in einem Brute–Force–Angriff, bei dem alle möglichen Schlüsselwörter durchprobiert werden. Immerhin könnten mit Hilfe moderner Computer, Wörter aus den 26 Buchstaben des Alphabets gebildet und diese zur Entschlüsselung des Kryptogramms herangezogen werden. Hinzu kommt, dass nicht alle der dadurch gewonnenen Texte ganz gelesen werden müssen. Schließlich erkennt man bereits nach wenigen Silben, ob diese einer natürlichen Sprache entsprechen oder nicht.

Diese Möglichkeit sollte im Unterricht gemeinsam mit den Schülern geprüft werden, da die junge, computerbegeisterte Generation häufig die Leistungsfähigkeit von Rechnern überschätzt. Die Grenze eines Brute–Force–Angriffs wird schnell deutlich, wenn man die Anzahl der möglichen Schlüsselwörter überprüft:

- Sollte ein Schlüsselwort aus zwei Buchstaben bestehen, kämen $26 \cdot 26 = 676$ Wörter in Betracht. Diese Anzahl ist noch relativ gering, kann aber in der Praxis ausgeschlossen werden, da ein so entstandener Geheimtext zu leicht gebrochen werden könnte.

- Geht man davon aus, dass das Schlüsselwort aus drei Buchstaben besteht, sind $26 \cdot 26 \cdot 26 = 17.576$ Möglichkeiten zu prüfen. Jeder mögliche Schlüssel liefert einen Text, der vom Angreifer persönlich auf seine Richtigkeit zu untersuchen ist.

- Ist bei den dreielementigen Buchstabenkombinationen kein vernünftiger Text entstanden, sind die Schlüsselwörter aus vier Buchstaben zu prüfen. Jetzt gibt es nochmals $26 \cdot 26 \cdot 26 \cdot 26 = 456.976$ mögliche Schlüssel.
- Konnte auch jetzt der Klartext nicht gefunden werden, sind bei den Schlüsselwörtern aus fünf Buchstaben schon über 11 Millionen Möglichkeiten zu untersuchen.

Nun wird deutlich, dass ein bloßes Durchprobieren aller möglichen Schlüsselwörter – selbst mit Computereinsatz – zu einem "endlosen" Unterfangen wird. Zum Entziffern muss deshalb eine andere Methode angewandt werden.

2. Kryptanalyse bei bekannter Länge des Schlüsselwortes
Im Unterricht sollte man zunächst die Kryptanalyse bei bekannter Länge des Schlüsselwortes durchführen. Dadurch erkennen die Schüler, dass zur Entschlüsselung die Länge des Schlüsselwortes eine entscheidende Rolle spielt und sind bestrebt, Methoden zum Auffinden der Schlüsselwortlänge zu erlernen.

Wie aus Abbildung 6.23 deutlich hervorgeht, werden bei der Länge n des Schlüsselwortes, die Buchstaben an den Positionen 1, n+1, 2n+1 usw. jeweils durch dasselbe Verschiebealphabet verschlüsselt. Die Buchstaben an den Positionen 2, n+2, 2n+2 usw. werden wiederum durch dasselbe Alphabet chiffriert. Analog schließt man auf die weiteren Buchstaben bis zur Position n, 2n, 3n usw.

Das zu entschlüsselnde Kryptogramm aus Abbildung 6.25 ist aus einem Schlüsselwort mit fünf Buchstaben hervorgegangen. Zur Kryptanalyse ist es nun hilfreich, das Kryptogramm (wie in der Abbildung) in Blöcke mit jeweils fünf Buchstaben einzuteilen. Dann kann man wie folgt vorgehen:

- Der erste Buchstabe eines jeden Blocks wurde durch dieselbe Caesar–Chiffre verschlüsselt. Folglich ermittelt man die relative Häufigkeit dieser Buchstaben. Der häufigste Buchstabe an der ersten Position eines jeden Blocks ist "F". Man kann folglich davon ausgehen, dass "F" für den Klartextbuchstaben "E" – dem häufigsten Buchstaben in der deutschen Sprache – steht. Die zugehörige Chiffre wäre dann

Klartextalphabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Geheimtextalphabet:	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Abbildung 6.26: Chiffre der ersten Buchstaben eines jeden Blocks

  Unterstützt wird diese Vermutung dadurch, dass der zweithäufigste Buchstabe an der ersten Position eines jeden Blocks "O" auch den in der deutschen Sprache am zweithäufigsten auftretenden Buchstaben "N" darstellt. Anhand dieser Erkenntnisse kann man davon ausgehen, dass jeder erste Buchstabe mit der zweiten Zeile des Vigenère–Quadrats verschlüsselt wurde und folglich das Schlüsselwort mit dem Buchstaben "B" beginnt.

- Analog zu oben ermittelt man nun die relative Häufigkeit jedes zweiten Geheimtextzeichens im Buchstabenblock. Hier stellt sich heraus, dass der Buchstabe "E" am häufigsten

vertreten ist, gefolgt vom Buchstaben "N". Da diese Auftrittswahrscheinlichkeit gerade der der natürlichen Sprache entspricht, wurde jeder zweite Buchstabe wahrscheinlich mit sich selbst verschlüsselt, d. h. mit der ersten Zeile im Vigenère–Quadrat. Damit wäre der zweite Buchstabe des Schlüsselwortes "A".

- Nun verfährt man ebenso mit den Buchstaben an der dritten, vierten und fünften Position in jedem Buchstabenblock. Über die relative Häufigkeit der Geheimtextzeichen erhält man das Alphabet, mit dem die entsprechenden Buchstaben substituiert wurden. Dieses Alphabet wiederum liefert den gesuchten Buchstaben des Schlüsselwortes. Im Unterricht sollten die Schüler zu diesem Zeitpunkt in der Lage sein, die noch fehlenden Buchstaben selbst zu ermitteln. Das gesuchte Schlüsselwort lautet für dieses Kryptogramm "Bauer".

Hat man das Schlüsselwort ermittelt, ist dieses – wie bei der Verschlüsselung – buchstabenweise unter das Kryptogramm zu notieren. Das Alphabet mit diesem Buchstaben in der ersten Spalte des Vigenère–Quadrats ist nun das Geheimtextalphabet, mit dem die Verschlüsselung stattgefunden hat. Zur Entschlüsselung sucht man im entsprechenden Verschiebealphabet das Geheimtextzeichen auf und erhält in der ersten Zeile über dem Geheimtextzeichen im Vigenère–Quadrat den Klartextbuchstaben. Im vorliegenden Kryptogramm lautet der so zu ermittelnde Klartext:
"Vor wenigen Jahren noch war die Kryptologie, die Lehre von den Geheimschriften und ihrer unbefugten Entzifferung, ein recht im Verborgenen blühender Zweig – blühend, weil von alters her ihre professionellen Vertreter gut ernährend"[22].

3. Kasiski–Test zum Auffinden der Länge des Schlüsselwortes
Wie im vorhergehenden Abschnitt geschildert, lässt sich bei bekannter Länge des Schlüsselwortes ein Vigenère–chiffriertes Kryptogramm entziffern. Nun geht es darum, die Länge des Schlüsselwortes mithilfe des Kasiski–Tests aufzufinden.

Ausgangspunkt dieser Methode ist, dass in einem Text bestimmte Wörter (wie z. B. der, die, den usw.) oder Wortteile (Trigramme) öfter auftreten. Im Allgemeinen werden diese bei der Vigenère–Verschlüsselung unterschiedlich chiffriert. Beträgt allerdings der Abstand zwischen diesen Wörtern bzw. Trigrammen gerade die Länge des Schlüsselwortes oder ein Vielfaches hiervon, werden diese Wörter gleich verschlüsselt (vgl. Abbildung 6.27):

Klartext:	V O R	W E N I G E N	J A H R E N ...	D I E	L E H R E ...
Schlüsselwort:	B A U	E R B A U E R	B A U E R B ...	U E R	B A U E R ...

Abbildung 6.27: Das Trigramm "HRE" von Jahre und Lehre wird gleich verschlüsselt.

Beim Kasiski–Test wird nun ein Kryptogramm nach gleichen Zeichenfolgen untersucht und der Abstand zwischen diesen Buchstaben ermittelt. Denn wenn diese Buchstabenkombinationen von gleichen Klartextbuchstaben hervorgerufen werden, ist der Abstand dieser Zeichenketten ein Vielfaches der Schlüsselwortlänge. Im Kryptogramm aus Abbildung 6.25 treten beispielsweise folgende gleiche Buchstabenkombinationen auf (vgl. Abbildung 6.28):

[22] [2], S. 2

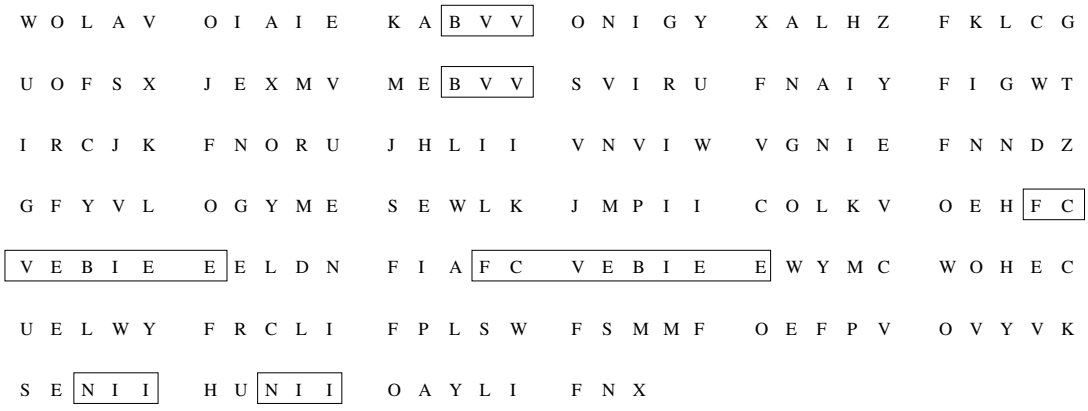


Abbildung 6.28: gleiche Buchstabenkombinationen im Kryptogramm

Dabei beträgt der Abstand zwischen der Zeichenfolge “BVV” 30, “FCVEBIEE” 15 und der Buchstabenkombination “NII” 5 Zeichen. Daraus ist zu schließen, dass die Schlüsselwortlänge sowohl ein Teiler von 30, 15 als auch von 5 sein muss. Eine Zerlegung der einzelnen Zahlen in ihre Primfaktoren liefert sofort das Ergebnis: das Schlüsselwort muss 5 Zeichen lang sein.

4. Erhöhung der Sicherheit von Vigenère–Chiffren
Nach der Behandlung der Kryptanalyse von Vigenère–Verschlüsselungen sollten im Unterricht auch Überlegungen zur Erhöhung der Sicherheit dieser Chiffren angestellt werden. Dadurch werden die Schüler nicht nur angeleitet, “geeignete” Schlüsselwörter zu finden. Eine derartige Unterrichtseinheit bereitet insbesondere auch auf das Thema “Perfekte Sicherheit” vor. Die Sicherheit von Vigenère–chiffrierten Kryptogrammen hängt wesentlich von der Länge des Schlüsselwortes ab. Wie beim Kasiski–Test aufgezeigt wurde, führt ein relativ kurzes Schlüsselwort zu mehr gleichen Buchstabenkombinationen im Chiffrat als ein langes Schlüsselwort. Insofern kann die Sicherheit durch die Verwendung sehr langer Schlüsselwörter erhöht werden. Bei der Suche nach langen Wörtern stoßen die Schüler jedoch schnell an ihre Grenzen. Deshalb wird nun dazu übergegangen, nicht nur ein Wort zu verwenden, sondern mehrere Wörter – die “Schlüsselwürmer”. Besonders sicher sind solche Schlüsselwürmer, die ebenso lang sind, wie die zu übermittelnde Nachricht.

Ein Problem im Zusammenhang mit der Verwendung von Schlüsselwürmern ist, dass diese zwischen den Kommunikationspartnern auf einem sicheren Weg ausgetauscht werden müssen. Um die Kosten der Übertragung in Grenzen zu halten, hat es sich in der Vergangenheit bewährt, auf Bücher zurückzugreifen. Die Kommunikationspartner vereinbaren ein Buch, dessen Text als Schlüssel dient und müssen beim Schlüsselaustausch lediglich die Seite und evtl. die Zeile mitteilen, auf der der Schlüsselwurm beginnen soll. Beispielsweise ergibt sich mit der Seite 10 von Julius Vernes “Reise zum Mittelpunkt der Erde” der Schlüsselwurm “MEINONKELWARFUEREINENDEUTSCHENPROFESSORREICH...” (vgl. Abbildung 6.29).

Eine andere Möglichkeit die Sicherheit von Vigenère–Verschlüsselungen zu erhöhen, besteht darin, anstelle von verschobenen Alphabeten im Vigenère–Quadrat permutierte Alphabete zu verwenden. Immerhin wurde durch die Beibehaltung der alphabetischen Reihenfolge der Geheimtextalphabete beim Kasiski–Test die Schlüsselsuche wesentlich vereinfacht. Dem steht

Klartext: V O R W E N I G E N J A H R E N N O C H W A R ...

Schlüssel: M E I N O N K E L W A R F U E R E I N E N D E ...

Abbildung 6.29: Der Klartext wird mit einem Schlüsselwurm chiffriert.

aber wiederum der Nachteil gegenüber, dass nicht nur ein Schlüssel, sondern auch das Vigenère–Quadrat zwischen den Kommunikationspartnern ausgetauscht werden müsste. Insofern rechtfertigt die dadurch gewonnene Erhöhung der Sicherheit den Mehraufwand beim Schlüsselaustausch kaum.

Der Journalist Robert Matthews veröffentlichte 1989 in [24] eine Bastelanleitung für ein einfaches Rotorgerät, das eine Vigenère–Verschlüsselung ermöglicht (siehe Anhang F auf Seite 163). Zum Abschluss des Themas "Vigenère–Verschlüsselung" und zur Vorbereitung auf die nächste Unterrichtseinheit über Rotormaschinen bietet sich im Unterricht der Bau dieses Verschlüsselungsgerätes an.

6.2.3.4 Rotormaschinen

In der Geschichte der Kryptographie weisen zahlreiche Erfindungen auf das Bestreben der Menschen hin, die Verschlüsselung zu mechanisieren:

Eine der ersten Chiffriergeräte ist die bereits 1466 von Leon Battista Alberti vorgestellte Chiffrierscheibe (siehe Seite 75). Der Chiffrierschieber, eine Gegenüberstellung von Klar- und Geheimtextalphabeten auf gegeneinander verschiebbaren Linealen, wurde um 1600 verwendet. Der Staatsmann Thomas Jefferson (1743 - 1826), der u. a. die amerikanische Unabhängigkeitserklärung mitformulierte und von 1801 bis 1809 dritter Präsident von Amerika war, erfand das nach ihm benannte Jefferson Rad, das eine polyalphabetische Verschlüsselung von 36 Zeichen in einem Schritt ermöglicht.

Ab etwa 1920 wurden schließlich Rotormaschinen, d. h. elektromechanische Chiffriermaschinen, entwickelt. Im Unterricht sollte hier aufgezeigt werden, inwiefern die polyalphabetische Substitution mithilfe von Rotormaschinen möglich ist und die bekannteste Rotormaschine, die Enigma, besprochen werden.

Intentionen

- Die Schüler sollen die Mechanisierung der polyalphabetischen Substitution mithilfe von Rotormaschinen beschreiben können.
- Die Schüler sollen in der Lage sein, die grundlegende Funktionsweise der Enigma zu erklären.

Inhalte
Bevor auf die Mechanisierung der polyalphabetischen Substitution eingegangen werden kann, ist im Unterricht zunächst die Funktionsweise einer monoalphabetischen Chiffriermaschine zu

erarbeiten. Dieses Prinzip ist in Abbildung 6.30 skizziert. Dabei wurde aus Gründen der Übersichtlichkeit das Alphabet auf die ersten sechs Buchstaben verkürzt.

Die Klartextbuchstaben (a, b, c, d, e, f) werden hierbei durch Schließen eines Schalters verschlüsselt. Wird der Schalter betätigt, fließt über Kontakte Strom zu einer Lampe, die mit dem entsprechenden Geheimtextzeichen versehen ist. Wie aus Abbildung 6.30 ersichtlich ist, wird z. B. der Buchstabe “d” durch das Zeichen “C” chiffriert.

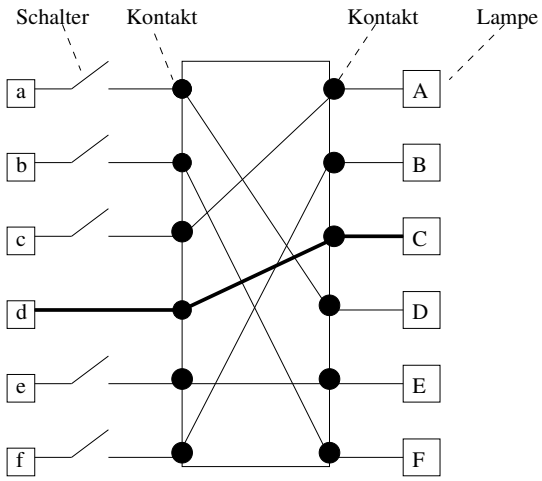


Abbildung 6.30: Bauplan einer monoalphabetischen Chiffriermaschine

Im Unterricht bietet es sich an, eine solche Chiffriermaschine als elektrische Schaltung zu bauen. Neben motivationalen und positiven fächerübergreifenden Auswirkungen zum Unterrichtsfach Physik, erkennen die Schüler an der Schaltung unmittelbar deren Funktionsweise.

Die vorgestellte Chiffriermaschine erleichtert zwar die Verschlüsselung, kann aber keinerlei Sicherheit bieten, da sie lediglich eine monoalphabetische Chiffrierung bewirkt. Die Buchstaben von “a” bis “f” werden hier wie folgt permutiert:

Klartextzeichen:	a b c d e f
Geheimtextzeichen:	D F A C E B

Abbildung 6.31: Permutation der Buchstaben durch die Chiffriermaschine

Dasselbe Ergebnis erhält man, wenn man die Verdrahtung zwischen den Kontakten nicht mehr auf einer Ebene anordnet, sondern zylinderförmig in einer Walze. Die Schalter mit den Klartextbuchstaben befinden sich am linken Ende der Walze, die Lampen mit den Geheimtextzeichen sind am rechten Ende der Walze befestigt (vgl. Abbildung 6.32). Abbildung 6.33 macht deutlich, wo sich die Kontakte befinden[23)].

Der entscheidende Vorteil der walzenförmigen Anordnung der Verdrahtung besteht darin, dass die Walze zwischen der Abdeckung mit den Schaltern (auf denen die Klartextbuchstaben stehen) und derjenigen mit den Lampen (an denen die Geheimtextzeichen stehen) gedreht werden

[23)] vgl. hierzu [20], S. 197 und [30], S. 162

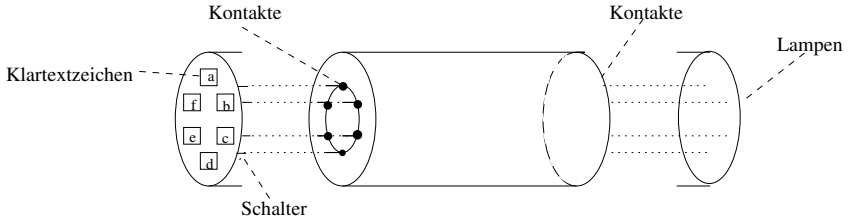


Abbildung 6.32: Zylinderförmige Anordnung der monoalphabetischen Chiffriermaschine

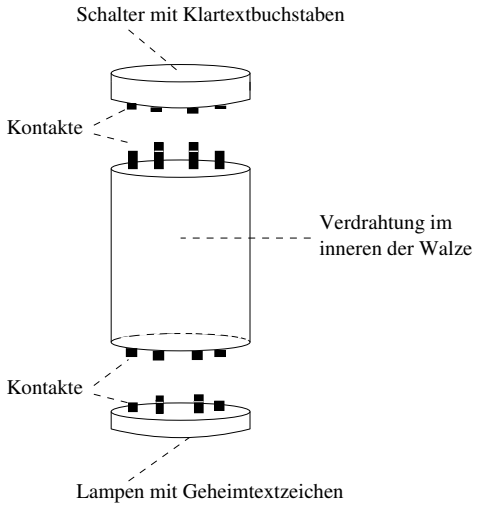


Abbildung 6.33: Anordnung der Kontakte an einer zylinderförmigen Chiffriermaschine

kann. Nach einer Drehung der Walze sind die Kontakte mit anderen Lampen verbunden. Dies ermöglicht den Übergang zur polyalphabetischen Chiffrierung.

Veranschaulichen kann man eine 1/6–Drehung der Walze dadurch, dass im Bauplan der monoalphabetischen Chiffriermaschine aus Abbildung 6.30 eine Verschiebung der rechteckigen Plattform mit den Kontakten um einen Kontakt nach oben vorgenommen wird. Der nun überhängende Kontakt vom Schalter a wird danach unten beim Buchstaben f angefügt. Die dadurch mögliche polyalphabetische Chiffrierung wird durch einen Vergleich der Permutationen der Klartextzeichen deutlich (vgl. Abbildung 6.34).

	ursprüngliche Permutation:	Permutation nach der "Verschiebung":
Klartextzeichen:	a b c d e f	a b c d e f
Geheimtextzeichen:	D F A C E B	E F B D A C

Abbildung 6.34: Permutation der Buchstaben vor und nach einer Verschiebung der Kontakte

Wird folglich bei einem Alphabet mit 26 Buchstaben nach jedem Klartextzeichen die Verdrahtung zwischen den festen Schalter- und Lampenkontakten der Rotormaschine um einen Kontakt gedreht, erhält man eine polyalphabetische Chiffrierung. Diese entspricht einer Vigenère–

Verschlüsselung mit permutierten Alphabeten. Nach einer vollen Umdrehung, d. h. nach 26 Zeichen findet eine Wiederholung der Geheimtextalphabete statt, was bei Vigenère einem Schlüsselwurm mit 26 Zeichen gleichkommt.

Da eine Chiffrierung auf Basis eines aus 26 Zeichen bestehenden Schlüsselwortes nicht sicher genug ist, wurden später Rotormaschinen mit mehreren Walzen entwickelt. Die Walzen sind dabei hintereinander angeordnet und mittels Kontakten miteinander verknüpft (vgl. Abbildung 6.35). Zur Verschlüsselung ist folglich die Verdrahtung in mehreren Walzen entscheidend.

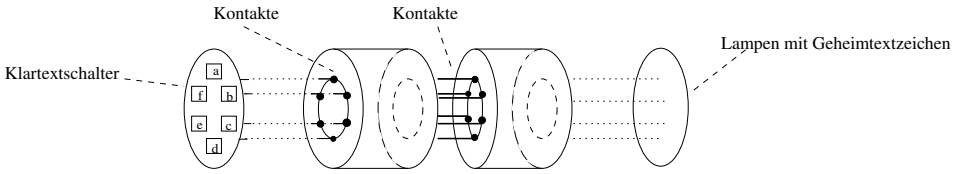


Abbildung 6.35: Rotormaschine aus zwei Walzen

Nach Verschlüsselung eines Buchstabens dreht sich die linke Schlüsselwalze um einen Kontakt weiter und verändert auf diese Weise die Zuordnung der Geheimtextzeichen für den nächsten Buchstaben. Nach einer vollen Umdrehung der linken Walze wird die rechte Walze um einen Kontakt gedreht. Man erhält dadurch für weitere 26 Buchstaben ein verändertes Geheimtextalphabet, wobei sich wiederum nur die linke Walze bewegen muss. Insgesamt werden auf diese Weise $26 \cdot 26 = 676$ Zuordnungen von Klar- und Geheimtextalphabeten ermöglicht; d. h. man erhält eine Vigenère ähnliche Verschlüsselung mit einem Schlüsselwurm von 676 Zeichen.

Auf analoge Weise bietet eine Rotormaschine mit drei Schlüsselwalzen 17576, eine mit vier Schlüsselwalzen 456976 und eine mit fünf Rädern über 11 Millionen mögliche Verschlüsselungen an.

Nachdem das Rotorprinzip behandelt ist, sollte im Unterricht auf die Chiffriermaschine Enigma eingegangen werden. Denn “die Enigma–Maschine steht einzigartig da. Keine andere Maschine begann ihr Dasein als gewöhnliche Handelsware und beendete es als eine Sache, die größten Einfluss auf den Ausgang eines interkontinentalen Konfliktes besaß”[24]. Des Weiteren zeigt sich am Beispiel der Enigma sehr deutlich, dass die Sicherheit eines kryptographischen Systems nicht einzig auf der Größe des Schlüsselraums beruht und gebrochen werden kann. Eine Tatsache, die die Deutschen lange Zeit für unmöglich gehalten hatten.

Schließlich lässt sich auch der Verlauf des Zweiten Weltkrieges aus einer neuen Perspektive beobachten. Mit der Enigma wurden nicht nur Funksprüche der Marine verschlüsselt, sondern auch sämtliche Vorhaben der deutschen Militärführung. Die Entschlüsselung ermöglichte es Großbritannien, alliierte Geleitzüge im Atlantik zu schützen und sich in der Luftschlacht um England auf Bombenangriffe vorzubereiten. Man erkennt, welchen großen Einfluss Geheimhaltung in Krisenzeiten inne hat.

[24] [23], S. 29

Enigma
Als Erfinder der Enigma gilt der deutsche Ingenieur Dr. Arthur Scherbius (1878 - 1929). Er meldete 1918 ein Patent für die Konstruktion einer Chiffriermaschine an, gründete 1923 die Chiffriermaschinen–Aktiengesellschaft und begann die Enigma kommerziell auf Messen als zivile Verschlüsselungsmaschine vorzustellen. Der Verkauf lief zunächst allerdings sehr schleppend. Der Chef der Heeresleitung, Generaloberst von Seeckt war schließlich der erste, der die militärische Bedeutung der Enigma erkannte. 1926 führte er die Enigma zuerst in der Marine ein und 1932 wurde das deutsche Heer mit der verbesserten Enigma I ausgestattet. Zeitgleich wurde das handelsübliche Modell vom Markt genommen.

Mit Einführung der Enigma im Militär, wurden Soldaten an einer Fernmeldeschule im Verschlüsseln und Entschlüsseln von Kryptogrammen ausgebildet. Der Aufbau der Enigma wird in [23] sehr eindrucksvoll aus der Sicht eines jungen Soldaten geschildert:
"Zunächst einmal sah er etwas, das wie eine plumpe, solide und primitive Schreibmaschine oder eine Kontrollkasse aussah. Vorne befand sich wie auf jeder gewöhnlichen Schreibmaschine ein Tastenfeld. Aber das erste, das der Auszubildende lernte, war, dass, wenn er z. B. die Taste mit dem Buchstaben X betätigte, kein X erschien, wie das normalerweise der Fall war. Dafür erblickte er auf dem flachen Oberteil der Maschine ein weiteres Alphabet. Wenn er nun die Taste X im Tastenfeld drückte, erschien nicht ein X, sondern ein anderer Buchstabe, zum Beispiel ein K, weil ein Licht ihn von unten beleuchtete. X war zu K geworden, und was bei diesem Ersetzen geschah, war das Rätsel, das die Enigma bot. Hier lag der Kernpunkt des deutschen Schlüsselsystems"[25)].

Nach dieser Einführung sind Schüler motiviert, mehr über "das Rätsel Enigma" zu erfahren, wodurch eine Überleitung zum Aufbau dieser Chiffriermaschine hergestellt ist. Die Enigma ist grundsätzlich eine Rotormaschine, die aus drei Schlüsselwalzen besteht. Wird ein Klartextbuchstabe gedrückt, wird – wie bei jeder Rotormaschine – ein elektrischer Kontakt hergestellt, der über die Verdrahtung dreier Schlüsselwalzen das Aufleuchten des Geheimtextzeichens bewirkt. Neben diesem Grundprinzip einer Rotormaschine weist die Enigma folgende zusätzliche Ausstattungen auf:

Nach der Verschlüsselung eines Buchstabens wird nicht nur eine Schlüsselwalze um einen Kontakt weitergedreht. Über ein Getriebe können sich alle Walzen um eine bestimmte Anzahl von Kontakten drehen und damit eine neuartige Verdrahtung erzeugen.

Neben den drei Schlüsselwalzen beinhaltet die Enigma eine Umkehrwalze, die auch als Reflektor bezeichnet wird. Diese befindet sich am Ende der drei Schlüsselwalzen, ist unbeweglich und schickt einen elektrischen Impuls auf einem anderen Weg wieder durch die drei Schlüsselwalzen zurück. Mit der Umkehrwalze wird erreicht, dass man mit derselben Chiffriermaschine sowohl ver- als auch entschlüsseln kann. Zur Entschlüsselung muss (bei gleicher Stellung der Walzen) nur das Kryptogramm eingetippt werden. Dann erscheinen der Reihe nach die Klartextbuchstaben im Lampenfeld (vgl. Abbildung 6.36)[26)].

[25)] [23], S. 36
[26)] vgl. hierzu [30], S. 167

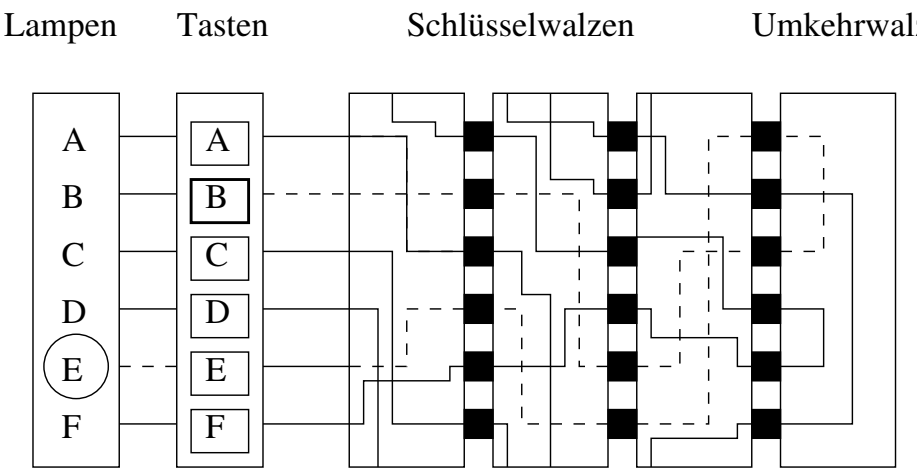


Abbildung 6.36: Funktionsweise der Enigma: Wird die Taste B gedrückt, durchläuft ein elektrischer Impuls drei Schlüsselwalzen, wird durch die Umkehrwalze auf einem anderen Weg zurückgeschickt und führt zum Aufleuchten des Buchstabens E. Umgekehrt erhält man beim Drücken der Taste E den Klartextbuchstaben B.

Eine weitere Besonderheit der Enigma ist, dass die Schlüsselwalzen aus der Maschine herausgenommen und in eine neue Stellung gebracht werden können. Damit kann die Verdrahtung und folglich auch die Verschlüsselung der Buchstaben in entscheidender Weise verändert werden.

Schließlich beinhaltet die Enigma noch das Steckerbrett. Damit können zwischen Tastatur und der ersten Schlüsselwalze Buchstaben vertauscht werden. So ist es möglich, insgesamt 6 Buchstabenpaare wie z. B. die Buchstaben A und C miteinander zu vertauschen. Bei der Verschlüsselung von A wird dann die Verdrahtung genutzt, die dem Buchstaben C zugeordnet ist und umgekehrt.

Wie bereits erwähnt, können sich nach einer Verschlüsselung mehrere Schlüsselwalzen um eine bestimmte Anzahl von Kontakten drehen. Diese Bewegung wird durch eine Kerbe auf einem Ring um eine Schlüsselwalze ausgelöst. Die Stellung des Rings auf der Walze kann auch verändert werden, was das unbefugte Entschlüsseln nochmals erschwert.

Zur Verschlüsselung musste folglich

- die Lage (d. h. die Reihenfolge) der Schlüsselwalzen,
- die Stellung der Schlüsselwalzen,
- die Ringstellung jeder Walze und
- die Steckerverbindungen

festgelegt werden. Diese Ausgangsstellung der Enigma entspricht dem Schlüssel, der für jeden Tag in einem Schlüsselbuch festgelegt wurde. Natürlich durfte dieses Schlüsselbuch nie in gegnerische Hände fallen.

Nach Besprechung der Einstellungsmöglichkeiten der Enigma sollte im Gymnasium die Anzahl der möglichen Schlüssel bestimmt werden (siehe Anhang G auf Seite 165). An Realschulen und Hauptschulen sind diese Berechnungen nicht geeignet, da im Lehrplan Stochastik nicht vorgesehen ist und damit kein Vorwissen hierin vorausgesetzt werden kann.

Bei der Größe des Schlüsselraumes der Enigma stimmt es verwunderlich, dass Chiffrate gebrochen werden konnten. Dies lag zum einen an Fehlern von deutschen Funkern, wie sie in [1] beschrieben werden, sowie an Verrat, Zufall und vor allem den Leistungen der Kryptoanalytiker in Polen um Marian Rejewski und in England um Alan Turing. Diese Ereignisse sind ausführlich in [30] und [23] beschrieben. Wie intensiv sie im Unterricht behandelt werden, bleibt der einzelnen Lehrkraft überlassen. In jedem Fall sollte noch eine Schwachstelle der Enigma untersucht werden, die Umkehrwalze.

Der Zweck der Umkehrwalze ist, dass mit derselben Maschine sowohl verschlüsselt, als auch Kryptogramme entschlüsselt werden können. Diesem Vorteil steht jedoch der Nachteil einer starken Einschränkung der möglichen Buchstabenpermutationen gegenüber. Dies lässt sich am Beispiel eines Alphabets mit vier Buchstaben (ABCD) veranschaulichen:

In Abbildung 6.37 sind alle $4! = 24$ möglichen Permutationen der vier Buchstaben ABCD aufgeführt.

A B C D	A B D C	A C B D	A C D B	A D B C	A D C B
B A C D	B A D C	B C A D	B C D A	B D A C	B D C A
C A B D	C A D B	C B A D	C B D A	C D A B	C D B A
D A B C	D A C B	D B A C	D B C A	D C A B	D C B A

Abbildung 6.37: Permutationen der Buchstaben ABCD

Die Umkehrwalze bewirkt zunächst, dass kein Buchstabe in sich selbst übergehen kann, da jeder elektrische Impuls auf einem anderen Weg durch die drei Schlüsselwalzen zurückgeschickt wird, als er gekommen ist. Betrachtet man die vier Buchstaben in alphabetischer Reihenfolge, werden folgende Zeichen in sich selbst überführt (vgl. Abbildung 6.38).

A B C D	A B D C	A C B D	A C D B	A D B C	A D C B
B A C D	B A D C	B C A D	B C D A	B D A C	B D C A
C A B D	C A D B	C B A D	C B D A	C D A B	C D B A
D A B C	D A C B	D B A C	D B C A	D C A B	D C B A

Abbildung 6.38: Die unterstrichenen Buchstaben werden bei der dargestellten Permutation in sich selbst übergeführt.

Nachdem Permutationen, bei denen ein Buchstabe in sich selbst übergeht, mit der Enigma nicht erzeugt werden können, sind diese für die folgenden Überlegungen zu streichen. Damit bleiben von ursprünglich 24 Möglichkeiten noch folgende 9 Permutationen übrig (vgl. Abbildung 6.39).

B A D C	B C D A	B D A C
C A D B	C D A B	C D B A
D A B C	D C A B	D C B A

Abbildung 6.39: Permutationen der vier Buchstaben ABCD ohne Identitäten.

Wie bereits erwähnt, kann aufgrund der Umkehrwalze ein Kryptogramm durch bloßes Eintippen in die Maschine entschlüsselt werden. Das bedeutet, dass bei zweimaliger Verschlüsselung der Klartext erzeugt wird. Ein bereits behandeltes Beispiel einer solchen Chiffre, ist das Verschlüsselungsverfahren ROT13 (siehe Seite 60). Auch hier erhält man bei zweimaliger Chiffrierung den Klartext. Im Fall der Enigma bedeutet dies, dass nur solche Permutationen ermöglicht werden, bei denen nach zweimaliger Anwendung der ursprüngliche Buchstabe erzeugt wird. Das hat eine weitere Einschränkung von möglichen Permutationen zur Folge. Wie in Abbildung 6.40 ersichtlich ist, erfüllen nur noch drei Permutationen diese Voraussetzung.

B A D C	B C D A	B D A C
C A D B	**C D A B**	C D B A
D A B C	D C A B	**D C B A**

Abbildung 6.40: Die umrandeten Permutationen können durch die Enigma erzeugt werden.

Insgesamt kann festgehalten werden, dass durch die Umkehrwalze die Anzahl der möglichen Permutationen des Alphabets erheblich reduziert und damit ein unbefugtes Entziffern erleichtert wird. Zudem ermöglicht die Verschlüsselung ohne Identitäten, dem unbefugten Angreifer die Suche nach wahrscheinlichen Wörtern. Trifft beim Erraten von Wörtern ein Geheimtextzeichen auf denselben Buchstaben des vermuteten Wortes, kann dieses ausgeschlossen werden.

Nachdem die Funktionsweise und die kryptographischen Schwächen der Enigma behandelt sind, empfiehlt sich, eine Simulation der Enigma im Unterricht einzusetzen[27)]. Zum einen bereitet es Schülern Freude, wenn sie am Computer die Verschlüsselung der Enigma vornehmen und testen können, zum anderen werden wichtige Lerninhalte wiederholt und gefestigt. Dazu gehören z. B.

- Festlegung der Einstellungen, die bei der Verschlüsselung mit der Enigma dem Schlüssel entsprechen.

[27)] Im Internet sind mehrere frei verfügbare Programme vorhanden, die die Enigma simulieren. Zum Beispiel eignet sich hiervon das Programm des Informatikers Marian Kassovic von der Universität Hamburg unter ftp://agn-www.informatik.uni-hamburg.de/pub/cryptsim/simulators/. Bei diesem können sämtliche Einstellungsmöglichkeiten der Enigma vorgenommen und die Bewegung der Rotoren während der Verschlüsselung direkt beobachtet werden. Zusätzlich besteht die Auswahl zwischen der im Unterricht behandelten Dreiwalzen– und einer Vierwalzenenigma.

- Verschlüsseln und anschließendes Entschlüsseln von Texten mit der Enigma, um vor Augen zu führen, dass die Enigma eine involutorische Chiffre erzeugt.

- Verschlüsseln eines Textes, der nur aus einem Buchstaben besteht, und anschließende Analyse des Kryptogramms. Besteht der Text beispielsweise nur aus den Buchstaben A, wird im Kryptogramm aufgrund der identitätsfreien Verschlüsselung kein A auftauchen. Damit erhält man Hinweise auf die interne Verdrahtung der Schlüsselwalzen, die zur Zeit des Einsatzes der Enigma geheim zu halten war. Diese Geheimhaltung der Verdrahtung entspricht einem Widerspruch zum Prinzip von Kerckhoffs (vgl. Seite 78), womit die Sicherheit der Enigma–Chiffre stark eingeschränkt werden muss. Tatsächlich gelang es den Kryptoanalytikern im Zweiten Weltkrieg durch Verrat und Fehler von deutschen Funkern, Hinweise auf die interne Verdrahtung der Walzen zu erlangen.

Aufgrund der hohen Behaltensleistung originärer Erfahrungen, sollte zum Abschluss des Themenbereichs “Rotormaschinen” ein Besuch des Deutschen Museums vorgenommen werden. In der Informatik–Abteilung ist ein eigener Bereich der Kryptographie gewidmet. Neben Erläuterungen zu den bisher im Unterricht behandelten Chiffren, sind vor allem Chiffriergeräte wie z. B. das Jefferson–Rad und die Enigma ausgestellt.

6.2.4 Perfekte Sicherheit

Den bisher behandelten Chiffrierverfahren ist gemeinsam, dass sie alle im Rahmen der Kryptanalyse gebrochen werden konnten. Allerdings ist festzustellen, dass die Chiffrierverfahren immer sicherer wurden und die Kryptoanalytiker im Laufe der Zeit einen zunehmenden Aufwand zum Brechen entsprechender kryptographischer Verfahren leisten mussten. Deshalb erhebt sich nun die Frage, unter welchen Bedingungen ein Chiffrierverfahren nicht mehr unbefugt entschlüsselt werden kann, d. h. perfekte Sicherheit gewährleistet.

Die Veranschaulichung der perfekten Sicherheit eines Kryptosystems soll anhand der Vernam–Chiffrierung erfolgen, dem Chiffrierverfahren, das beweisbar perfekte Geheimhaltung ermöglicht. Voraussetzung hierfür ist allerdings, Buchstaben als Zahlen darzustellen. Besonderer Wert wird dabei auf der praxisbezogenen Darstellung von Zeichen durch Dualzahlen gelegt.

Intentionen

- Die Schüler sollen in der Lage sein, Buchstaben durch (Dual-) Zahlen darzustellen.

- Die Schüler sollen die Chiffrierung nach Vernam durchführen können.

- Die Schüler sollen in der Lage sein, die perfekte Sicherheit anhand der Vernam–Chiffrierung zu erläutern.

- Die Schüler sollen Möglichkeiten für die Erzeugung von Zufallszahlen nennen können.

6.2.4.1 Darstellung von Buchstaben durch Zahlen

An dieser Stelle wird thematisiert, dass Verschlüsselungen wie z. B. die Vigenère–Chiffre in der Praxis nicht mit Buchstaben, sondern mit Zahlen vorgenommen werden. Dadurch erhebt sich die Frage, wie Buchstaben als Zahlen dargestellt werden können. Neben einem einfachen Durchnummerieren der Buchstaben von 01 bis 26, sollten im Unterricht weitere Methoden aufgezeigt werden. In dieser Arbeit wird eine antike Möglichkeit nach Polybius sowie die praxisrelevante Darstellung der Buchstaben in Form des ASCII–Codes[28)] vorgeschlagen.

Die Einführung des ASCII–Codes ist aufgrund seiner praktischen Bedeutung unabdingbar[29)]. Da bei diesem allerdings eine Nummerierung der Buchstaben in alphabetischer Reihenfolge stattfindet, dient die Polybius–Chiffre dazu, den Schülern nicht nur eine antike, sondern auch eine völlig andere Methode aufzuzeigen, wie Buchstaben als Zahlen dargestellt werden können.

Polybius–Chiffre
Dem griechischen Historiker Polybius[30)] wird zugeschrieben, eine Chiffre entwickelt zu haben, in der Buchstaben durch zweistellige Zahlen verschlüsselt werden. Bei dieser Chiffre wird das Alphabet (ohne den Buchstaben J) in eine 5x5–Matrix einbeschrieben und ein Buchstabe durch Angabe seiner Zeilen- und Spaltenkoordinaten chiffriert.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Abbildung 6.41: Polybius–Matrix

Wie aus Abbildung 6.41 ersichtlich ist, wird beispielsweise der Buchstabe P durch 35, der Buchstabe O durch 34 usw. chiffriert. Auf diese Weise erhält man aus dem Wort “Polybius” die Zahlenfolge:

35 34 31 54 12 24 45 43.

Man erkennt, dass eine ursprünglich monoalphabetische Chiffre dazu verwendet werden kann, Buchstaben in Form von Zahlen darzustellen.

[28)] American Standard Code for Information Interchange

[29)] Der ASCII–Code umfasst nicht nur das lateinische Alphabet in Groß- und Kleinschreibung, sondern auch Ziffern sowie einige Satz- und Steuerzeichen. Die elektronische Datenverarbeitung bei Computern erfolgt weitgehend auf Grundlage des ASCII–Codes.

[30)] Polybius – um 200 v. Chr. auf dem Peloponnes geboren – verfasste in 40 Bänden eine Historie von der Zeit um 220 bis 146 v. Chr. Von seinem Werk sind die ersten fünf Bücher überliefert, in denen überwiegend der Aufstieg Roms zur Weltmacht dargelegt wird.

ASCII–Code
Eine der frühsten Formen der Kodierung war der, in der ersten Hälfte des 19. Jahrhunderts, in der Telegrafie angewandte Morsecode. Dieser wurde vom 1870 entwickelten Baudot–Code ersetzt, der alle Zeichen durch einen Code fester Länge darstellt. Der Baudot–Code bildet die Grundlage für den ASCII–Code, der jedes Zeichen durch einen 7–Bit–Code festlegt (siehe Seite 167). Die heute vorherrschende Kodierung von Buchstaben erfolgt durch den ASCII–Code.

Bei Einführung des ASCII–Codes sollten im Unterricht sowohl die Dezimal– als auch die Dualwerte entsprechender Zeichen vorgestellt werden. In diesem Zusammenhang sollte das Dualsystem – auch Binärsystem oder Zweiersystem genannt – eingeführt werden. An Realschulen wird das Dualsystem als Stellenwertsystem zur Basis 2, sowie die Umrechnungen vom Dezimal- zum Dualsystem und umgekehrt, bereits im Mathematikunterricht der 5. Jahrgangsstufe eingeführt, so dass hier eine kurze Wiederholung genügt.

6.2.4.2 Vernam–Chiffrierung

Anknüpfend an die Überlegungen zur Sicherheit der Vigenère–Chiffre (siehe Seite 83) wird im Unterricht wiederholt, dass bei Verwendung eines "Schlüsselwurms", d. h. mehrerer aneinander geschriebener Wörter, die Vigenère–Verschlüsselung einen besonders hohen Sicherheitsgrad erreicht. In diesem Fall ist das Schlüsselwort ebenso lang wie der Klartext. Da dieses allerdings aus Wörtern einer natürlichen Sprache besteht, ist die unbefugte Kryptanalyse aufgrund bestimmter Sprachmuster – wie Buchstabenhäufigkeiten, Häufigkeiten von Bigrammen und Trigrammen – möglich.

Der amerikanische Ingenieur des Telekommunikationskonzerns AT&T Gilbert Sanford Vernam veröffentlichte 1917 die Idee, ebenfalls mithilfe eines unendlich langen Schlüssels zu chiffrieren. Im Gegensatz zur obigen Überlegung sollte dieser Schlüssel jedoch aus Zufallszahlen bestehen. Umgesetzt wurde diese Idee 1918 durch den amerikanischen Kryptologen und Generalmajor in der US–Armee Joseph Oswald Mauborgne.

Bei diesem Verfahren wird der Klartext als Zahlenfolge dargestellt und ziffernweise mit einem Schlüssel derselben Länge chiffriert, indem Klartextzahl und Schlüsselzahl (ohne Übertrag) addiert werden. Da somit Klartext und Schlüssel "zusammenfließen", bezeichnet man dieses Verfahren auch als Fluss- oder Stromchiffrierung (vgl. Abbildung 6.42).

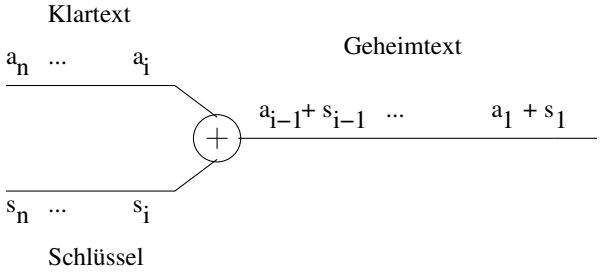


Abbildung 6.42: Die Flusschiffre

1921 stießen auch der Mathematiker Werner Kunze, der Kryptologe Rudolf Schauffler und der Chemiker Erich Langlotz – die von der Nationalversammlung der Weimarer Republik den Auftrag erhalten hatten, ein Chiffrierverfahren für den diplomatischen Dienst zu entwickeln – auf diese kryptographische Methode. Für die Umsetzung in der Praxis wurden Blöcke mit zufällig gewählten Zahlen bedruckt, die als Schlüssel verwendet wurden. Da jede Zahlenfolge nur einmal verwendet werden durfte, musste nach einer Chiffrierung das benutzte Blatt vernichtet werden. Aufgrund der Anwendung eines Blocks mit Zufallszahlen, die nur einmal Verwendung finden, bezeichnet man diese Chiffre auch als "one–time pad".

Einigen sich nun zwei Kommunikationspartner auf die Verschlüsselung nach Vernam, benötigt man zunächst zwei identische Blöcke mit zufällig gewählten Zahlen, von denen sowohl der Sender als auch der Empfänger der Nachrichten jeweils einen erhält. Die Vernam–Chiffrierung findet dann in folgenden Schritten statt:

- Die Buchstaben des Klartextes werden nach einem vereinbarten Verfahren als Zahlen dargestellt.
- Unter diese Zahlenfolge werden die Zufallszahlen nach der Vorgabe des Bocks notiert.
- Die Zahlen des Klartextes und des Schlüssels werden ohne Zehnerübertrag addiert. Das Ergebnis stellt den Geheimtext dar.
- Das verwendete Blatt mit den Zufallszahlen sowie sämtliche Aufzeichnungen werden vernichtet und der Geheimtext an den Empfänger geschickt.

Im Unterricht ist dieses Verfahren an einem Beispiel zu veranschaulichen (vgl. Abbildung 6.43). Der Klartext "Ausbruch heute Nacht" wird zuerst mit dem ASCII-Code als Zahlenfolge dargestellt. Die Zahlen des Schlüssels wurden zufällig gewählt und zu den Zahlen des Klartextes ohne Zehnerübertrag addiert.

Klartext:	Ausbruch heute Nacht
ASCII–Code:	651171159811411799104104101117116101789799104116
Schlüssel:	103387210379430061942546658720201106018037963342
Kryptogramm:	754458369180841750046640759837317207797726067458

Abbildung 6.43: Beispiel einer Vernam–Chiffrierung

Im Unterricht sollte nach einer Übung der Vernam–Chiffrierung im Zehnersystem auch die entsprechende Verschlüsselung im Dualsystem eingeführt werden. Denn zum einen wird dieses kryptographische Verfahren heute vor allem bitweise betrieben, zum anderen hat Vernam diese Chiffre dazu entwickelt, um die Nachrichtenübermittlung in der Telegrafie zu verschlüsseln. Die Buchstaben wurden zu dieser Zeit mit Hilfe des Baudot–Codes als Folge von Dualzahlen dargestellt und sowohl der Klartext als auch der Schlüssel, in Form von Lochstreifen in den

Telegrafenapparat eingelesen. Dabei bedeutete ein “Loch” die Zahl Eins und “kein Loch” stellte die Zahl Null dar.

Die Vernam–Verschlüsselung im Dualsystem (vgl. Abbildung 6.44) erfolgt analog zur Verschlüsselung im Zehnersystem, indem die Addition ohne Übertrag erfolgt, d. h. nach der Regel:

$$0+0 = 0\ ,\ 1+0 = 1\ ,\ 0+1 = 1\ ,\ 1+1 = 0.$$

Klartext:	Maus
ASCII–Code:	01001101011000010111010101110011
Schlüssel:	00101001110110111101001001000100
Geheimtext:	01100100101110101010011100110111

Abbildung 6.44: Beispiel einer Vernam–Chiffrierung im Dualsystem

Entschlüsselt wird, indem vom Geheimtext der Schlüssel nach folgender Regel subtrahiert wird:

$$0\text{-}0 = 0\ ,\ 1\text{-}0 = 1\ ,\ 0\text{-}1 = 1\ ,\ 1\text{-}1 = 0.$$

Im nächsten Kapitel wird gezeigt, dass ein unbefugter Dechiffrierer keine Möglichkeit hat, einen Vernam–chiffrierten Geheimtext zu entschlüsseln, sofern zwei Bedingungen erfüllt sind:

- Der Schlüssel besteht aus zufällig gewählten Zahlen.
- Der Schlüssel wird nur einmal verwendet.

Man spricht in diesem Fall von perfekter Geheimhaltung bzw. von perfekter Sicherheit.

6.2.4.3 Perfekte Sicherheit

Für eine exakte Erläuterung des Begriffs “Perfekte Sicherheit” sind grundlegende Kenntnisse aus der Wahrscheinlichkeitsrechnung erforderlich. Schüler an Hauptschulen und Realschulen weisen hierin kein Vorwissen auf. Deshalb sollte an diesen Schulen auf eine Definition des Begriffs “Perfekte Sicherheit” zugunsten einer Veranschaulichung anhand der Vernam–Chiffrierung verzichtet werden.

An Gymnasien ist Stochastik im Lehrplan des Mathematikunterrichts enthalten. Folglich verfügen Gymnasiasten über genügend Vorwissen, um den Begriff der “Perfekten Sicherheit” exakt zu erfassen. Aus diesem Grund wird hier eine intensivere Behandlung dieses Themas vorgeschlagen, wie unter dem Abschnitt “Perfekte Sicherheit eines Kryptosystems” vorgestellt wird.

Veranschaulichung der Perfekten Sicherheit
Intuitiv bedeutet perfekte Sicherheit, dass sich bei Kenntnis des Geheimtextes, keine Informa-

tionen über den Klartext ergeben. Diese Vorstellung von perfekter Geheimhaltung lässt sich an einem Beispiel der Vernam–Chiffrierung aufzeigen.

Angenommen, der in Abbildung 6.45 angegebene Teil eines Geheimtextes gelangt in die Hände einer unbefugten Person. Analog zum Prinzip nach Kerckhoffs soll bekannt sein, dass zur Verschlüsselung das Verfahren nach Vernam angewandt wurde.

Da der Schlüssel aus einer Folge von zufällig gewählten Zahlen besteht, hat eine unbefugte Person keine Möglichkeit, aus dem Kryptogramm Hinweise für den Schlüssel zu erhalten. Damit bleibt nur noch die Möglichkeit, Schlüsselfolgen zu erraten. Abbildung 6.45 zeigt nun auf, dass es für einen Geheimtext unendlich viele Möglichkeiten für Schlüssel und zugehörige Klartexte gibt. Ein Kryptogramm kann mit entsprechenden Schlüsseln in jeden gleich langen Text übersetzt werden. Ohne Kenntnis des Schlüssels hat damit eine unbefugte Person keine Möglichkeit, aus dem Kryptogramm Hinweise auf den zugrunde liegenden Klartext zu gewinnen.

Geheimtext:	01100100101110101010011100110111	
Schlüssel 1:	00101001110110111101001001000100	
Klartext 1:	01001101011000010111010101110011	ASCII–Code für Maus
Schlüssel 2:	00101100110011111100100101010011	
Klartext 2:	01001000011101010110111001100100	ASCII–Code für Hund
Schlüssel 3:	00100010110101101100100001011111	
Klartext 3:	01000110011011000110111101101000	ASCII–Code für Floh

Abbildung 6.45: Ohne Kenntnis des Schlüssels kann der Geheimtext nicht entziffert werden.

Perfekte Sicherheit eines Kryptosystems
Um den Begriff "Perfekte Sicherheit" erfassen zu können, ist zunächst zu definieren, was unter einem Kryptosystem zu verstehen ist. Aus diesem Grund sind im Unterricht folgende Begriffe einzuführen:

Analog zu den Anfangsbuchstaben der Wörter Klartext, Geheimtext und Schlüssel werden folgende Bezeichnungen festgelegt und an unten stehendem Beispiel erläutert:

- K ist die Menge aller Klartexte.
- G ist die Menge aller Geheimtexte bzw. Kryptogramme.
- S ist die Menge aller Schlüssel.

Für das Beispiel in Abbildung 6.46 gilt entsprechend:

- K besteht aus den Klartexten a, b, c; d. h. K = {a, b, c}.
- G besteht aus den Geheimtexten w, x, y, z; d. h. G = {w, x, y, z}.

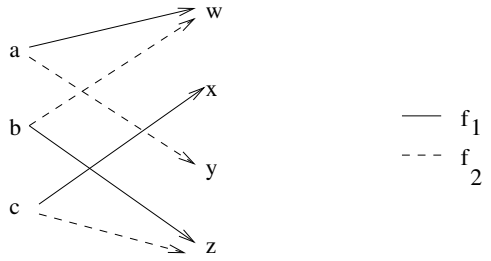


Abbildung 6.46: Beispiel von Verschlüsselungsverfahren

- Die durch Pfeile dargestellten Verschlüsselungsfunktionen werden mit f_1 und f_2 bezeichnet. Die Indizes 1 und 2 stehen für die Schlüssel. Im Beispiel gilt:

$$f_1(\text{a}) = \text{w}$$
$$f_2(\text{a}) = \text{y}$$
$$f_1(\text{b}) = \text{z}$$
$$\ldots$$

  Die Menge aller Schlüssel S besteht folglich aus 1 und 2. Damit gilt S = {1, 2}.

Damit ein Kryptogramm entschlüsselt werden kann, müssen die Verschlüsselungsfunktionen umkehrbar sein. Die zur Verschlüsselungsfunktion f_s gehörende Entschlüsselungsfunktion bezeichnet man (analog zur Umkehrfunktion) mit f_s^{-1}. Im obigen Beispiel gilt:

$$f_1^{-1}(\text{w}) = \text{a}$$
$$f_2^{-1}(\text{y}) = \text{a}$$
$$f_1^{-1}(\text{z}) = \text{b}$$
$$\ldots$$

Nun kann im Unterricht festgelegt werden, was unter einem Kryptosystem zu verstehen ist. Dazu wird die Definition nach Claude E. Shannon[31)] herangezogen.

Ein Kryptosystem besteht aus

1. einer Menge K von Klartexten,
2. einer Menge G von Geheimtexten,
3. einer Menge S von Schlüsseln,
4. einer Menge von umkehrbaren Verschlüsselungsfunktionen und
5. einer Menge von Entschlüsselungsfunktionen, so dass gilt:

$$f_s^{-1}(f_s(k)) = k \text{ für alle } k \in \text{K}.$$

[31)] Claude Elwood Shannon (1916 - 2001) war amerikanischer Mathematiker und gilt als Begründer der Informationstheorie.

Bevor der Begriff “Perfekte Sicherheit” definiert wird, sollten die Begriffe der “bedingten Wahrscheinlichkeit” und der “Unabhängigkeit von Ereignissen” wiederholt werden. Dazu eignen sich die folgenden Definitionen:

- Sind A und B Ereignisse und P(B) > 0. Die Wahrscheinlichkeit für “A unter der Bedingung B” ist definiert als
$$P(A|B) = \frac{P(A \cap B)}{P(B)}.$$
- Zwei Ereignisse A und B heißen unabhängig, wenn gilt:
$$P(A \cap B) = P(A)P(B).$$

Nun lässt sich der Begriff “Perfekte Sicherheit eines Kryptosystems” definieren und anschließend auch erläutern:

Ein Kryptosystem heißt perfekt sicher, falls die Ereignisse, dass ein bestimmter Geheimtext auftritt und ein bestimmter Klartext vorliegt, unabhängig sind, d. h. P(k|g) = P(k) für alle k $\in$ K und alle g $\in$ G.

Erläuterungen:

- Falls die Ereignisse k und g unabhängig sind, erhält man
$$P(k|g) = \frac{P(k \cap g)}{P(g)} = \frac{P(k) \cdot P(g)}{P(g)} = P(k).$$
- Wäre P(k|g) > P(k) für einen Klartext k, dann würde der unbefugte Dechiffrierer durch Analyse von g feststellen, dass mit hoher Wahrscheinlichkeit k vorliegt.
- Wäre P(k|g) < P(k) für einen Klartext k, dann würde durch Analyse von g der Klartext k ausgeschlossen werden können. Dies darf bei perfekter Sicherheit nicht möglich sein.

6.2.4.4 Auffinden von Zufallszahlen

Die perfekte Sicherheit beruht bei der Vernam–Chiffre im Wesentlichen auf der Tatsache, dass der Schlüssel aus Zufallszahlen besteht. Im Unterricht sollten deshalb Möglichkeiten erörtert werden, wie Zufallszahlen erzeugt bzw. aufgefunden werden können.

Folgen echter Zufallszahlen können z. B. auf folgende Weisen erzeugt werden:

- Werfen einer Münze zur Erzeugung einer Folge von Dualzahlen. Dabei kann “Kopf” für die Zahl 0 und “Zahl” für 1 stehen.
- Werfen eines Würfels mit der benötigten Augenzahl.
- Ziehen von Kugeln, auf denen Zahlen stehen, aus einer Urne mit Zurücklegen.

Da diese Verfahren sehr zeitaufwändig sind, werden in der Praxis häufig Folgen von pseudozufälligen Zahlen herangezogen. Abbildung 6.47 zeigt ein Schieberegister der Länge 4, mit dem Pseudozufallszahlen erzeugt werden können. Außer dem Schieberegister benötigt man eine Initialisierung, d. h. für jede Zelle eine Ziffer. Daneben ist eine Rückkopplung erforderlich, die für die erste Zelle nach jedem Schritt eine neue Zahl liefert. In Abbildung 6.47 wird eine neue Zahl für die erste Zelle durch Addition (ohne Übertrag) der Werte in den Zellen zwei und vier gewonnen. Wird die Rückkopplung durch Addition vorgenommen, spricht man von linearen Schieberegistern.

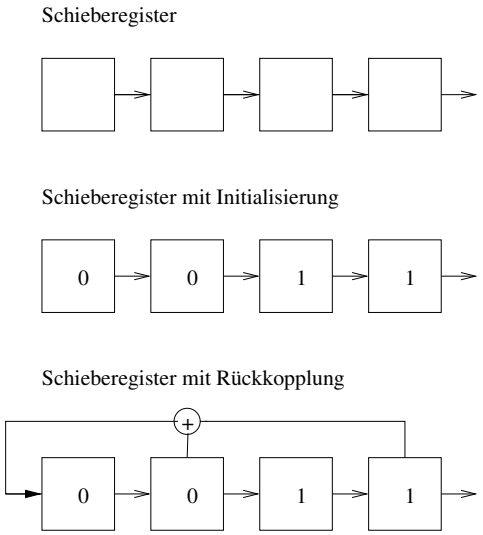


Abbildung 6.47: Beispiel eines Schieberegisters der Länge 4 mit der Initialisierung 0011 und einer linearen Rückkopplung

Der Nachteil linearer Schieberegister zeigt sich schnell, wenn man die von obigem Schieberegister erzeugte Folge von Zufallszahlen analysiert:

... 0011110011110011

Bereits nach sechs Zahlen findet eine Wiederholung statt. Eine Vernam–Chiffre, die auf einer periodischen Pseudozufallsfolge basiert, bietet allerdings nicht mehr Sicherheit, als eine Vigenère–Verschlüsselung. Deshalb sind Schieberegister, die brauchbare Pseudozufallszahlen erzeugen, nichtlinear zu konstruieren. Für die Rückkopplung werden hierbei auch Multiplikationen herangezogen. Ein Beispiel eines nichtlinearen Schieberegisters zeigt Abbildung 6.48.

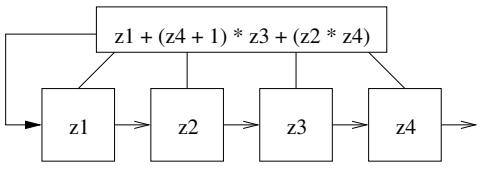


Abbildung 6.48: Beispiel eines nichtlinearen Schieberegisters der Länge 4

Neben der Zeitersparnis bieten Schieberegister den Vorteil, dass zwischen den Kommunikationspartnern nicht der gesamte Schlüssel ausgetauscht werden muss. Es genügt, das Schieberegister und dessen Initialisierung zu vereinbaren, um dieselben Pseudozufallszahlen zu erzeugen. Weitere Möglichkeiten für Pseudozufallszahlen mit entsprechender Vereinfachung des Schlüsselaustauschs sind z. B.:

- Die Kommunikationspartner einigen sich auf eine irrationale Zahl und die Stelle, ab der die unendliche, nichtperiodische Dezimalbruchentwicklung als Schlüssel dienen soll.

- Die Kommunikationspartner können statistische Jahrbücher, Telefonbücher etc. heranziehen, um eine Pseudozufallsfolge zu erschaffen. So könnte man z. B. im Telefonbuch einer bestimmten Stadt ab einem vereinbarten Namen jede 3. und 5. Stelle der Telefonnummern als Pseudozufallsfolge heranziehen.

6.2.5 Zusammenfassung

In diesem Kapitel wird eine Unterrichtssequenz über symmetrische Chiffrierverfahren vorgestellt. Ausgehend von der Verschiebechiffre nach Caesar werden zunächst monoalphabetische Chiffrierverfahren behandelt. Durch Transpositionen lernen die Schüler anschließend ein Verschlüsselungsverfahren kennen, das die Klartextbuchstaben beibehält und nur deren Position verändert. Nach Einführung einer kryptographischen Methode wird stets auch die Sicherheit dieser Chiffre überprüft. Auf diese Weise werden die Schüler nicht nur in der Kryptanalyse geschult, sie erkennen auch die Schwächen der einzelnen Verschlüsselungsverfahren und stellen Überlegungen zu deren Verbesserung an.

Im Themenbereich der polyalphabetischen Chiffrierverfahren weisen die Verschlüsselungen eine zunehmende Sicherheit auf, was mit einem erhöhten Aufwand in der Kryptanalyse einhergeht. Da Rotormaschinen auch polyalphabetisch arbeiten, wird in diesem Zusammenhang eine Unterrichtssequenz über die Funktionsweise und die geschichtlichen Hintergründe der Enigma vorgeschlagen.

Die zunehmende Sicherheit polyalphabetischer Chiffren gipfelt schließlich in der Vernam–Verschlüsselung, die im Kapitel “Perfekte Sicherheit” behandelt wird.

Zusammenfassend kann festgehalten werden, dass bei allen vorgestellten kryptographischen Methoden die Vertraulichkeit von Nachrichten im Vordergrund stand. Ein Vergleich mit den Zielen den Kryptographie (siehe Seite 51) zeigt allerdings, dass damit nur eines von insgesamt vier Zielen angestrebt wurde. Inwiefern Nachrichtenintegrität und Authentizität von Nachrichten und Kommunikationspartnern mit den Methoden der symmetrischen Chiffrierverfahren erreicht werden kann, wird im Kapitel 6.4 auf Seite 127ff erörtert.

6.3 Asymmetrische Chiffrierverfahren

Symmetrische Chiffrierverfahren sind dadurch gekennzeichnet, dass sowohl zum Chiffrieren als auch zum Dechiffrieren der gleiche Schlüssel existiert, der zuvor zwischen den Kommunikationspartnern auf einem sicheren Weg ausgetauscht werden muss. Bei asymmetrischen Verfahren ist dieser sichere Schlüsselaustausch nicht erforderlich, da diese auf Grundlage eines Schlüsselpaares für jeden Teilnehmer beruhen:

- einem öffentlichen, frei verfügbaren Schlüssel zum Chiffrieren einer Nachricht und
- einem privaten, geheimen Schlüssel zum Dechiffrieren eines Kryptogramms.

Analog zur symmetrischen Verschlüsselung sollte auch die Funktionsweise asymmetrischer Chiffrierverfahren anhand einer Grafik verdeutlicht werden (vgl. Abbildung 6.49).

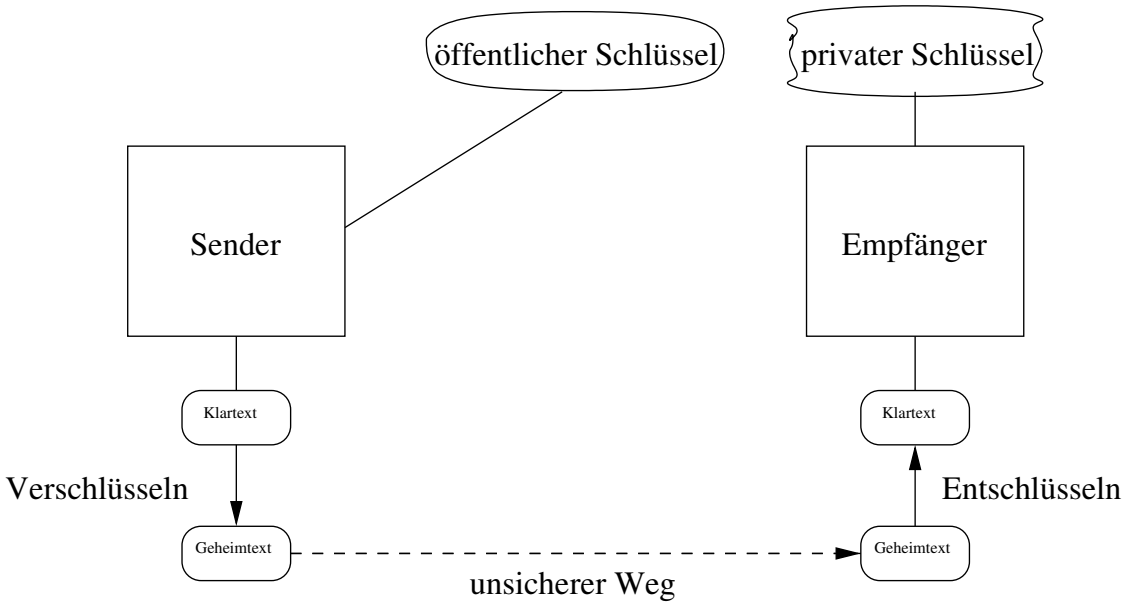


Abbildung 6.49: Verfahren der asymmetrischen Verschlüsselung

Die asymmetrische Verschlüsselung erfolgt beim Versenden einer Nachricht in vier Schritten:

- Der Sender einer Nachricht sucht sich den öffentlichen Schlüssel des Kommunikationspartners z. B. aus einem öffentlichen Schlüsselverzeichnis heraus.
- Mithilfe des öffentlichen Schlüssels chiffriert der Sender eine Nachricht und erhält den zugehörigen Geheimtext.
- Das Kryptogramm kann nun auf einem unsicheren Weg an den Empfänger der Nachricht geschickt werden.
- Der Empfänger wendet zum Dechiffrieren der Nachricht seinen privaten (geheimen) Schlüssel an und erhält dadurch den Klartext der Botschaft.

Veranschaulichen kann man die asymmetrische Verschlüsselung mit einem Briefkasten. Jeder kann in den Briefkasten einer bestimmten Person eine Nachricht hineinwerfen. Aber nur der Eigentümer des Briefkastens hat den Schlüssel, mit dem er diesen öffnen und die Briefe herausholen kann.

Aufgrund der dargelegten Funktionsweise weisen asymmetrische Chiffrierverfahren im Vergleich zu symmetrischen Verfahren folgende Vorteile auf:

- Vor dem Chiffrieren ist kein Schlüsselaustausch nötig.
- Man braucht im Gegensatz zu symmetrischen Verfahren nur sehr wenig Schlüssel (vgl. hierzu Anhang I auf Seite 168).
- Einige asymmetrische Verfahren bieten die Möglichkeit einer elektronischen Unterschrift (vgl. hierzu Kapitel 6.4 auf Seite 127ff).

Diesen Vorteilen stehen allerdings auch Nachteile der asymmetrischen Verfahren gegenüber:

- Asymmetrische Chiffrierverfahren sind mit hohem Rechenaufwand verbunden, was sich negativ auf die Übertragungsgeschwindigkeit der Nachrichten auswirkt.
- Um Missbrauch zu verhindern, ist eine Schlüsselverwaltung nötig, die garantiert, dass die öffentlichen Schlüssel authentisch sind und nicht von einem Dritten verändert wurden.

6.3.1 Modulo–Rechnung

Voraussetzung für die unterrichtliche Behandlung asymmetrischer Chiffrierverfahren ist die Einführung der Modulo–Rechnung, die sowohl für das RSA–Chiffrierverfahren als auch für die Schlüsselvereinbarung nach Diffie und Hellman von zentraler Bedeutung ist.

Intentionen

- Die Schüler sollen die Definition von “Kongruenzen” formulieren können.
- Die Schüler sollen in der Lage sein, die Modulo–Rechnung an Beispielen anzuwenden.

Inhalte
Bevor das Rechnen mit Resten eingeführt wird, ist die Definition der Teilbarkeit zu wiederholen. Zum Beispiel eignet sich hierzu folgende Formulierung:

Eine ganze Zahl $a \in \mathbb{Z}$ heißt durch eine Zahl $b \in \mathbb{Z}$ teilbar, wenn es eine ganze Zahl k gibt, so dass gilt

$$a = k \cdot b.$$

Bereits von der Grundschule ist bekannt, dass sich bei der Division von nicht teilbaren ganzen Zahlen ein Rest ergibt. Dieser Rest ist nun Gegenstand der Modulo–Rechnung, die anhand der Definition von “Kongruenzen” einzuführen ist.

"Es sei m eine natürliche Zahl mit $m > 1$. Lassen zwei ganze Zahlen a und b bei Division durch m den gleichen Rest, so nennt man a und b kongruent modulo m und schreibt dafür $a \equiv b \bmod m$"[32].

Im Unterricht ist diese Definition anhand von Beispielen zu erläutern. So gilt z. B. $1 \equiv 17 \bmod 4$ und $5 \equiv 23 \bmod 6$ usw. Untersucht man eine Vielzahl dieser Beispiele, so fällt auf, dass die Kongruenz $a \equiv b \bmod m$ genau dann gilt, wenn m die Differenz $b - a$ teilt. Dies ist auch leicht im Unterricht zu beweisen:

Es gelte $a \equiv b \bmod m$. Damit gilt:

$$\begin{aligned} \text{I} \quad & a = k_1 \cdot m + r \\ \text{II} \quad & b = k_2 \cdot m + r \end{aligned}$$

Die Differenz II - I der Gleichungen ergibt:

$$b - a = (k_2 - k_1) \cdot m.$$

Nach Definition der Teilbarkeit gilt damit $m|(b - a)$.

Gilt umgekehrt $m|(b - a)$, dann gibt es eine ganze Zahl k mit

$$\begin{aligned} & k \cdot m = b - a \\ \Leftrightarrow \quad & b = k \cdot m + a. \end{aligned}$$

Folglich lässt b bei Division durch m denselben Rest wie die Zahl a. Damit ist die Äquivalenz

$$a \equiv b \bmod m \Leftrightarrow m|(b - a) \tag{6.1}$$

bewiesen.

Um den Umgang mit der Modulo–Rechnung zu üben, sollten die folgenden Regeln mit den entsprechenden Beweisen im Unterricht behandelt werden. Die Rechenregel (6.3) findet außerdem zur Berechnung der diskreten Exponentialfunktion im nächsten Kapitel Anwendung.

Rechenregeln: Für $g_1, g_2, m \in \mathbb{N}$ gilt:

$$(g_1 + g_2) \bmod m \equiv (g_1 \bmod m) + (g_2 \bmod m) \tag{6.2}$$

$$(g_1 \cdot g_2) \bmod m \equiv (g_1 \bmod m) \cdot (g_2 \bmod m) \tag{6.3}$$

Beweis:
Seien $g_1 = k_1 m + r_1$ und $g_2 = k_2 m + r_2$. Dann gelten die Gleichungen

$$g_1 \bmod m \equiv r_1 \text{ und} \tag{6.4}$$

$$g_2 \bmod m \equiv r_2 \tag{6.5}$$

[32] [18], S. 315

sowie

$$\begin{aligned} k_1 m &= g_1 - r_1 \text{ und} \\ k_2 m &= g_2 - r_2. \end{aligned}$$

Zählt man die letzteren beiden Gleichungen zusammen, erhält man

$$(k_1 + k_2)m = (g_1 + g_2) - (r_1 + r_2).$$

Folglich ist m ein Teiler der Differenz $(g_1 + g_2) - (r_1 + r_2)$, womit nach (6.1)

$$(g_1 + g_2) \bmod m \equiv r_1 + r_2$$

gilt. Nach (6.4) und (6.5) gilt damit

$$(g_1 + g_2) \bmod m \equiv (g_1 \bmod m) + (g_2 \bmod m),$$

womit (6.2) bewiesen ist.

Um die Gleichung (6.3) zu beweisen, ist zunächst das Produkt $g_1 \cdot g_2$ zu betrachten. Es gilt:

$$\begin{aligned} g_1 \cdot g_2 &= (k_1 m + r_1) \cdot (k_2 m + r_2) \\ &= k_1 k_2 m^2 + k_1 r_2 m + k_2 r_1 m + r_1 r_2 \\ &= (k_1 k_2 m + k_1 r_2 + k_2 r_1) \cdot m + r_1 r_2 \\ \Leftrightarrow g_1 \cdot g_2 - r_1 \cdot r_2 &= (k_1 k_2 m + k_1 r_2 + k_2 r_1) \cdot m. \end{aligned}$$

Da folglich m ein Teiler der Differenz $g_1 g_2 - r_1 r_2$ ist, gilt nach (6.1)

$$(g_1 \cdot g_2) \bmod m \equiv r_1 \cdot r_2$$

und mit (6.4) und (6.5) erhält man

$$(g_1 \cdot g_2) \bmod m \equiv (g_1 \bmod m) \cdot (g_2 \bmod m),$$

womit (6.3) bewiesen ist.

6.3.2 Einweg–Funktionen mit Falltüre

Intentionen

- Die Schüler sollen die Notwendigkeit von Einwegfunktionen für asymmetrische Kryptosysteme erkennen.
- Die Schüler sollen Merkmale von Einwegfunktionen (mit Falltüre) beschreiben können.
- Die Schüler sollen Beispiele für Einwegfunktionen nennen können.
- Die Schüler sollen die Einweg–Eigenschaft der Produktbildung großer Primzahlen erkennen.

- Die Schüler sollen in der Lage sein, Funktionswerte der diskreten Exponentialfunktion zu bestimmen.
- Die Schüler sollen Verfahren und Aufwand zur Berechnung des diskreten Logarithmus kennen lernen.

Inhalte
Asymmetrische Chiffrierverfahren mit öffentlichen Schlüsseln erfordern, dass die Berechnung der Umkehrung der Verschlüsselungsfunktion praktisch nicht möglich ist. Man spricht in diesem Fall von "Einweg–Funktionen". Damit aber dem berechtigten Kommunikationspartner die Dechiffrierung möglich wird, werden Einweg–Funktionen mit Falltüre zur Verschlüsselung herangezogen.

"Eine injektive Funktion $f : X \to Y$ heißt Einwegfunktion mit Falltür, falls die folgenden Bedingungen gelten:

1. Es gibt effiziente Verfahren zur Berechnung von f und f^{-1}.
2. Das effiziente Verfahren zur Berechnung von f^{-1} kann aus f nicht ohne eine geheimzuhaltende Zusatzinformation gewonnen werden."[33)]

Die geheimzuhaltende Zusatzinformation stellt die Falltüre dar und entspricht dem privaten Schlüssel eines Teilnehmers.

Ein bekanntes Beispiel einer Einwegfunktion ist, zu einem Namen aus einem Telefonbuch einer bestimmten Stadt die Telefonnummer anzugeben. Das Nachschlagen der Telefonnummer ist sehr schnell möglich. Die Umkehrung hierzu, d. h. zu einer Telefonnummer den Namen der entsprechenden Person herauszusuchen, ist nur sehr schwer und mit erheblichem Zeitaufwand möglich.

Ein weiteres Beispiel einer Einwegfunktion ist die Überprüfung der Zugangsberechtigung an Computern mithilfe eines Passwortes. Ein Passwort ist im Rechner chiffriert gespeichert. Für einen Benutzer ist die Eingabe des Passwortes sehr einfach möglich. Nach dessen Eingabe wird das Passwort verschlüsselt und mit dem abgespeicherten Datensatz verglichen. Sind beide Kryptogramme identisch, wird der Zugang gewährt. Die Umkehrung zu diesem Vorgang wäre, bei Kenntnis des chiffrierten Passwortes, den Zugang zum Computer zu erlangen – bei Verwendung eines sicheren kryptographischen Verfahrens eine kaum zu lösende Aufgabe.

Die asymmetrische Kryptographie beruht auf zwei Einwegfunktionen mit Falltüre, die im Anschluss an die einleitenden Beispiele zu behandeln sind.

6.3.2.1 Produktbildung großer Primzahlen

Da man sich in der Schule im Wesentlichen mit kleinen Zahlen befasst, mag es für Schüler erstaunlich klingen, dass die Multiplikation großer Primzahlen eine Einwegfunktion darstellt.

[33)] [18], S. 328

Der Grund hierfür ist, dass die Produktbildung auch großer Zahlen vergleichsweise einfach ist. Bis heute sind allerdings keine effizienten Verfahren für die Primfaktorzerlegung bekannt.

Die Einweg–Eigenschaft der Produktbildung zweier Primzahlen lässt sich eindrucksvoll experimentell mit einem Computeralgebrasystem nachweisen.

Experimentelle Erfassung des Zeitaufwands beim Faktorisieren großer Zahlen
In dieser Arbeit wird der Einsatz des freien, open–source Computeralgebrasystems SAGE vorgeschlagen, das S. Müller–Stach in [25] vorstellt. SAGE steht für "System for Algebra and Geometry Experimentation" und bietet neben einer einfachen Bedienung den Vorteil, dass interessierte Schüler dieses auch zu Hause kostenlos verwenden können[34)].

Zur Veranschaulichung der Einweg–Eigenschaft der Produktbildung von Primzahlen wird den Schülern ein Arbeitsblatt mit Zahlen vorgegeben, die durch Multiplikation zweier, annähernd gleich großer Primzahlen hervorgegangen sind. Die Zahlen sind dabei nach Anzahl der Dezimalstellen aufsteigend geordnet. Nach einer Einführung in die Bedienung von SAGE besteht die Aufgabe der Schüler darin, die Rechenzeit für die Faktorisierung dieser Zahlen festzustellen.

In folgender Tabelle ist für eine Auswahl von Zahlen die Rechenzeit aufgeführt. Die erste Spalte zeigt die zu faktorisierende Zahl, die zweite Spalte gibt die Anzahl der Dezimalstellen dieser Zahl an und in der dritten Spalte ist die Rechenzeit in Sekunden auf einem "AMD Athlon XP 2400+" angegeben.

Zeitaufwand in Sekunden beim Faktorisieren von Zahlen mit SAGE		
Zahl	Stellen	Zeit [s]
68983	5	0,00
6891641177	10	0,00
669894887213567	15	0,00
24906222631629798763	20	0,01
3583909786265357067665203	25	0,02
57209150992949147229804114 7049	30	0,04
34289157531123382625083217419969097	35	0,11
15864376431028676287110934861389461202 89	40	0,37
24491538768566515025251423102771163771 3401871	45	1,38
28196714996164014899540472235411854518 136689282509	50	5,50
40130322124357826449863441276628361802787 27652963144233	55	15,04
29189630677843008385239072484932556713851 1950006696051290853	60	53,21
28052112020613036412374754567227735044660949868374216839979107801	65	178,42

Erstellt man aus diesen Werten ein Diagramm, wird sofort ersichtlich, dass die Rechenzeit mit zunehmender Anzahl von Dezimalstellen exponentiell ansteigt (vgl. Abbildung 6.50).

Um die Einweg–Eigenschaft der Produktbildung zu belegen, ist an dieser Stelle wichtig, auch den Zeitaufwand festzuhalten, um zwei Primzahlen miteinander zu multiplizieren. SAGE liefert das 65-stellige Ergebnis von

$$729019485746333354927695876030 49 \cdot 384792348751757985630987654321649$$

[34)] SAGE ist unter http://modular.ucsd.edu/sage erhältlich.

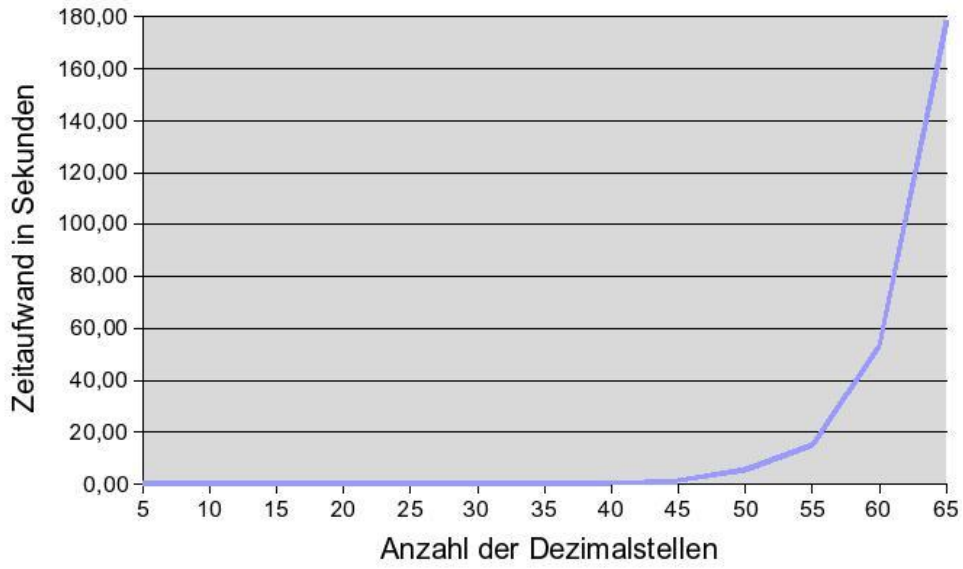


Abbildung 6.50: Veranschaulichung der gemessenen Zeiten beim Faktorisieren von Zahlen

in 0,00 Sekunden.

Nun ist deutlich, dass zwei sehr große Primzahlen schnell miteinander multipliziert werden können. Deren Faktorisierung ist jedoch nur mit großem Aufwand möglich. Auf dieser Einweg–Eigenschaft der Produktbildung beruht das später zu behandelnde asymmetrische RSA–Verfahren.

Eine weitere Einwegfunktion mit Falltüre stellt die diskrete Exponentialfunktion dar, deren unterrichtliche Einführung im folgenden Kapitel dargestellt wird.

6.3.2.2 Diskrete Exponentialfunktion

Gegeben seien die Zahlen $n \in \mathbb{N}$, $a \in \{0; 1; ...; n-1\}$ und ein Element $g \in \{0; 1; ...; n-1\}$. Die diskrete Exponentialfunktion ist definiert als

$$a \rightarrow g^a \bmod n.$$

Die diskrete Exponentialfunktion liefert folglich den Rest bei Division von g^a durch n. Im Unterricht ist anhand von Beispielen zunächst zu untersuchen, wie schnell die diskrete Exponentialfunktion berechnet werden kann.

Im Folgenden wird das Beispiel $4^8 \bmod 13$ auf unterschiedliche Weisen berechnet.

- Die erste und zugleich aufwändigste Möglichkeit $4^8 \bmod 13$ zu berechnen, ist, zuerst $4^8 = 65536$ zu bestimmen und anschließend den Rest bei Division durch 13 zu ermitteln. Man erhält auf diese Weise das Ergebnis 3.

- Die zweite Möglichkeit wendet zur Berechnung die Gesetzmäßigkeit

$$(g_1 \cdot g_2) \bmod n \equiv (g_1 \bmod n) \cdot (g_2 \bmod n)$$

an[35)]. Dann ist die Berechnung auch im Kopf mit 7 Multiplikationen modulo 13 möglich.

$$\begin{aligned} 4^8 \bmod 13 \equiv 4 \cdot 4^7 \bmod 13 &\equiv 4 \cdot 4 \cdot 4^6 \bmod 13 \\ &\equiv 3 \cdot 4 \cdot 4^5 \bmod 13 \\ &\equiv 12 \cdot 4 \cdot 4^4 \bmod 13 \\ &\equiv 9 \cdot 4 \cdot 4^3 \bmod 13 \\ &\equiv 10 \cdot 4 \cdot 4^2 \bmod 13 \\ &\equiv 1 \cdot 4 \cdot 4 \bmod 13 \\ &\equiv 4 \cdot 4 \bmod 13 \equiv 3. \end{aligned}$$

  Mithilfe dieser Berechnungsmethode kann die diskrete Exponentialfunktion $g^a \bmod n$ mit $a - 1$ Multiplikationen modulo n relativ schnell berechnet werden, da große Zahlen vermieden werden.

- Die dritte und schnellste Möglichkeit zur Berechnung des obigen Beispiels liefert der "Square and Multiply"–Algorithmus. Unter Verwendung der Potenzgesetze erhält man:

$$4^8 \bmod 13 \equiv (4^2)^4 \bmod 13 \equiv ((4^2)^2)^2 \bmod 13.$$

  Damit lässt sich die Berechnung in folgenden Schritten durchführen:

$$\begin{aligned} 4^8 \bmod 13 \equiv ((4^2)^2)^2 \bmod 13 &\equiv ((4^2 \bmod 13)^2 \bmod 13)^2 \bmod 13 \\ &\equiv (3^2 \bmod 13)^2 \bmod 13 \\ &\equiv 9^2 \bmod 13 = 3 \end{aligned}$$

  Zur Berechnung sind auf diese Weise lediglich 3 Multiplikationen modulo 13 notwendig. Dabei ist zu beachten, dass der "Square and Multiply"–Algorithmus auch bei solchen Potenzen angewandt werden kann, deren Exponent keine Zweierpotenz ist. Zum Beispiel ist a^{41} mithilfe der Potenzgesetze wie folgt darstellbar

$$a^{41} = a^{32+8+1} = a^{32} \cdot a^8 \cdot a,$$

  womit jeder Faktor eine Zweierpotenz als Exponenten erhält und obige Berechnungsmethode wieder möglich ist.

Zusammenfassend gilt damit, dass die diskrete Exponentialfunktion $g^a \bmod n$ selbst bei sehr großen Werten für den Exponenten a relativ schnell berechnet werden kann, da durch geeignete Verfahren sowohl große Zahlen vermieden werden können, als auch die Anzahl der notwendigen Multiplikationen reduziert und folglich der Rechenaufwand stark begrenzt werden kann.

Anhand von Beispielen wird nun gezeigt, dass die diskrete Exponentialfunktion nicht notwendigerweise injektiv ist, d. h. dass Elemente der Wertemenge mehrmals als Funktionswert angenommen werden können.

[35)] siehe Seite 104

Funktionswerte der diskreten Exponentialfunktion					
$2 \bmod 7$	$2^2 \bmod 7$	$2^3 \bmod 7$	$2^4 \bmod 7$	$2^5 \bmod 7$	$2^6 \bmod 7$
2	4	1	2	4	1
$4 \bmod 7$	$4^2 \bmod 7$	$4^3 \bmod 7$	$4^4 \bmod 7$	$4^5 \bmod 7$	$4^6 \bmod 7$
4	2	1	4	2	1

Wie die Tabelle unten zeigt, nimmt für bestimmte g die diskrete Exponentialfunktion $g^a \bmod n$ für alle $a \in \{1; 2; ...; n-1\}$ unterschiedliche Funktionswerte an. In diesem Fall wird g als Primitivwurzel mod n bezeichnet. Man kann zeigen, dass für jede Primzahl mindestens eine Primitivwurzel existiert. Beispielsweise sind die Zahlen 3 und 5 Primitivwurzeln für $n = 7$, wie nachfolgende Tabelle belegt.

Funktionswerte der diskreten Exponentialfunktion					
$3 \bmod 7$	$3^2 \bmod 7$	$3^3 \bmod 7$	$3^4 \bmod 7$	$3^5 \bmod 7$	$3^6 \bmod 7$
3	2	6	4	5	1
$5 \bmod 7$	$5^2 \bmod 7$	$5^3 \bmod 7$	$5^4 \bmod 7$	$5^5 \bmod 7$	$5^6 \bmod 7$
5	4	6	2	3	1

Wenn nun g eine Primitivwurzel ist, ist die diskrete Exponentialfunktion injektiv; folglich existiert eine Umkehrfunktion. Diese wird als diskrete Logarithmusfunktion bezeichnet und ist bedeutend schwerer zu berechnen. Für die Schule wird folgende Definition des diskreten Logarithmus vorgeschlagen:

Gegeben sei eine Primzahl p und ein Element $A \in \{1; 2; ...; p-1\}$. Sei g eine Primitivwurzel mod p. Der diskrete Logarithmus ist die Lösung $a \in \{0; 1; ...; p-2\}$ der Gleichung

$$g^a \equiv A \bmod p.$$

Nach dieser Einführung des diskreten Logarithmus ist im Unterricht dessen Berechnung zu erläutern. Ziel ist es, dass die Schüler erkennen, dass der Rechenaufwand zur Bestimmung des diskreten Logarithmus wesentlich höher ist, als derjenige zur Berechnung der diskreten Exponentialfunktion.

Obwohl es zur Bestimmung des diskreten Logarithmus schnellere Verfahren als bloßes Ausprobieren gibt, wird für den Unterricht letztere Methode vorgeschlagen. Denn auch die anspruchsvollen schnelleren Algorithmen wie z. B. das Babystep–Giantstep–Verfahren sind für die in der Praxis eingesetzten großen Primzahlen ineffizient. Insofern führt bereits die Methode des sukzessiven Erratens der Lösung zum gewünschten Lernerfolg und ist zudem leicht verständlich.

Um den diskreten Logarithmus durch Ausprobieren zu bestimmen, berechnet man schrittweise

$$A_1 \equiv g \bmod p;\ A_2 \equiv g^2 \bmod p;\ A_3 \equiv g^3 \bmod p; ...$$

bis man auf $A_k = A$ für ein $k \in \{0; 1; ...; p-2\}$ stößt.

Der Rechenaufwand für dieses – auch als Enumeration bezeichnete – Verfahren wird am besten an einem einfachen Beispiel deutlich:

Gegeben sei das diskrete Logarithmusproblem

$$14^a \equiv 7 \bmod 19.$$

Zur Lösung benötigt man folgende Rechenschritte:

$$\begin{aligned} 14 \bmod 19 &\equiv 14 \\ 14^2 \bmod 19 &\equiv 6 \\ 14^3 \bmod 19 &\equiv 8 \\ 14^4 \bmod 19 &\equiv 17 \\ 14^5 \bmod 19 &\equiv 10 \\ 14^6 \bmod 19 &\equiv 7 \end{aligned}$$

Das Beispiel macht deutlich, dass zur Lösung des diskreten Logarithmus $g^a \equiv A \bmod p$ insgesamt $a - 1$ Multiplikationen modulo p und a Vergleiche notwendig sind. Werden folglich – wie in kryptographischen Verfahren üblich – für a Werte über 2^{160} gewählt, ist diese Methode zur Lösung des diskreten Logarithmus praktisch nicht mehr durchführbar.

6.3.3 Diffie–Hellman–Schlüsselaustausch

Ein großer Nachteil symmetrischer Chiffrierverfahren ist der sichere Schlüsselaustausch zwischen den Kommunikationspartnern. Mit dem Diffie–Hellman–Schlüsselaustausch wird dieser Mangel behoben, da die Kommunikationspartner auch über einen unsicheren Kanal einen Schlüssel vereinbaren können. Das Diffie–Hellman–Verfahren ist folglich keine Verschlüsselungsmethode an sich. Es erleichtert vielmehr die Verwendung symmetrischer Verschlüsselungen durch einen vereinfachten, öffentlichen Austausch der geheimen Schlüssel.

Intentionen

- Die Schüler sollen in der Lage sein, den Ablauf des Diffie–Hellman–Schlüsselaustausches zu beschreiben.
- Die Schüler sollen anhand von Beispielen den Schlüsselaustausch nach Diffie und Hellman durchführen können.
- Die Schüler sollen die Sicherheit des Diffie–Hellman–Schlüsselaustausches richtig beurteilen können.

Inhalte
Der Diffie–Hellman–Schlüsselaustausch soll zunächst allgemein vorgestellt und anschließend an Beispielen erläutert werden. Hierzu werden die Kommunikationspartner – wie in der wissenschaftlichen Literatur üblich – mit Alice und Bob bezeichnet.

Um einen gemeinsamen Schlüssel K zu erzeugen, müssen sich Alice und Bob zunächst auf eine Primzahl p und eine Primitivwurzel g mod p mit $1 < g < p - 1$ einigen. Beide gewählte Zahlen können öffentlich bekannt sein.

Der Schlüsselaustausch erfolgt wie in Abbildung 6.51 dargestellt:

- Alice und Bob wählen je eine geheime Zahl a bzw. b aus $\{0; 1; ...; p-2\}$. Anschließend berechnet Alice $A = g^a \bmod p$, und Bob ermittelt $B = g^b \bmod p$.
- Die beiden Ergebnisse A und B werden an den jeweiligen Kommunikationspartner geschickt. Wichtig ist zu betonen, dass der Austausch der Zahlen A und B über einen unsicheren Kanal möglich ist, d. h. dass ein unbefugter Dritter diese Zwischenergebnisse in Erfahrung bringen kann, ohne den Schlüssel zu finden.
- Alice erhält durch die Berechnung von $B^a \bmod p$ denselben Wert wie Bob durch die Berechnung von $A^b \bmod p$. Dieser Wert stellt folglich den gemeinsamen Schlüssel dar.

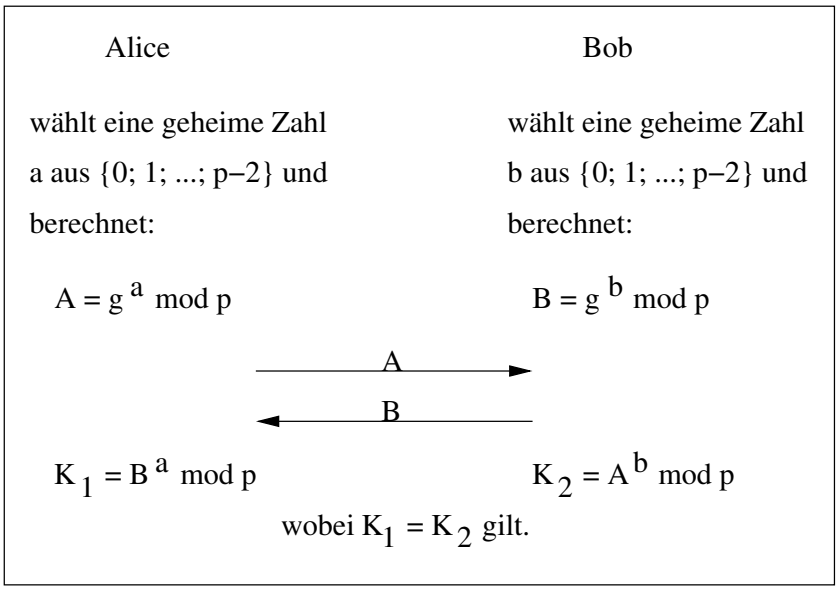


Abbildung 6.51: Der Diffie–Hellman–Schlüsselaustausch

Nun sind im Unterricht zwei Fragen zu klären:

- Wieso gilt $K_1 = K_2$?
- Kann der Schlüssel bei Kenntnis der Zahlen $g; p; A$ und B gefunden werden?

Die erste Frage ist einfach zu beantworten. Unter Anwendung der Potenzgesetze erhält man:

$K_1 = B^a \bmod p = (g^b \bmod p)^a \bmod p = (g^{ab}) \bmod p = (g^a \bmod p)^b \bmod p = A^b \bmod p = K_2$.

Folglich stellt $K_1 = K_2$ für die Kommunikationspartner den gemeinsamen geheimen Schlüssel dar.

Die zweite Frage ist unter Einbeziehung des Kapitels “Diskrete Exponentialfunktion” zu beantworten. Um den Schlüssel zu finden, müsste ein unbefugter Dritter “$g^{ab} \bmod p$” berechnen können. Dies setzt voraus, dass er aus den beiden Gleichungen

$$A = g^a \bmod p \quad \Leftrightarrow g^a = A \bmod p \quad \text{und}$$
$$B = g^b \bmod p \quad \Leftrightarrow g^b = B \bmod p$$

die Zahlen a und b berechnen, d. h. den diskreten Logarithmus bestimmen kann. Wie im vorherigen Kapitel dargelegt, ist diese Berechnung mit erheblichen Rechenaufwand verbunden und für entsprechend hohe Werte nicht mehr durchführbar.

An dieser Stelle sollten im Unterricht konkrete Rechenbeispiele wie in Abbildung 6.52 durchgeführt werden.

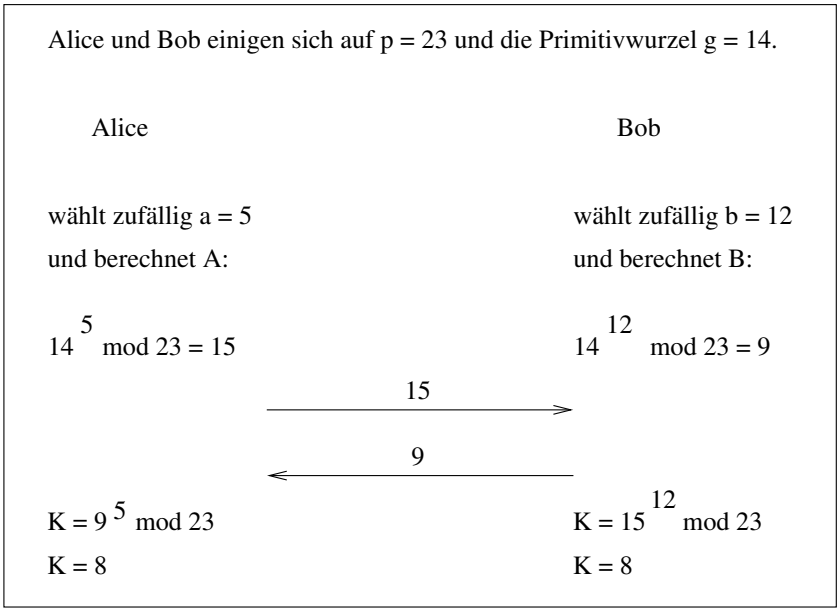


Abbildung 6.52: Beispiel eines Diffie–Hellman–Schlüsselaustausches

Im Unterricht bietet es sich auch an, dass zwei Schüler die Rolle von Alice und Bob übernehmen, einen gemeinsamen Schlüssel austauschen und die Zahlen angeben, die öffentlich bekannt sein können. Die Mitschüler erhalten die Aufgabe, den gemeinsamen Schlüssel zu finden. Schnell wird deutlich, dass bei "größeren" Zahlen die Berechnung zu aufwändig und nicht mehr durchführbar ist.

Sicherheit des Diffie–Hellman–Schlüsselaustausches
Die Sicherheit des Diffie–Hellman–Schlüsselaustausches hängt im Wesentlichen davon ab, dass das diskrete Logarithmusproblem nicht in akzeptabler Zeit gelöst werden kann. Sollte ein Verfahren entwickelt werden, mit dem diskrete Logarithmen effizient berechnet werden können, ist auch das Diffie–Hellman–Verfahren nicht mehr sicher.

Ein möglicher Angriff auf den Diffie–Hellman–Schlüsselaustausch stellt der in Rechnernetzen mögliche "Man–in–the–Middle" Angriff dar. Während Alice und Bob davon ausgehen, direkt miteinander zu kommunizieren, fängt ein unberechtigter Dritter – im Folgenden als "Charly" bezeichnet – die Nachrichten von Alice und Bob ab und sendet an beide Kommunikationspartner seine eigene Zahl zur Erstellung eines gemeinsamen Schlüssels (vgl. Abbildung 6.53).

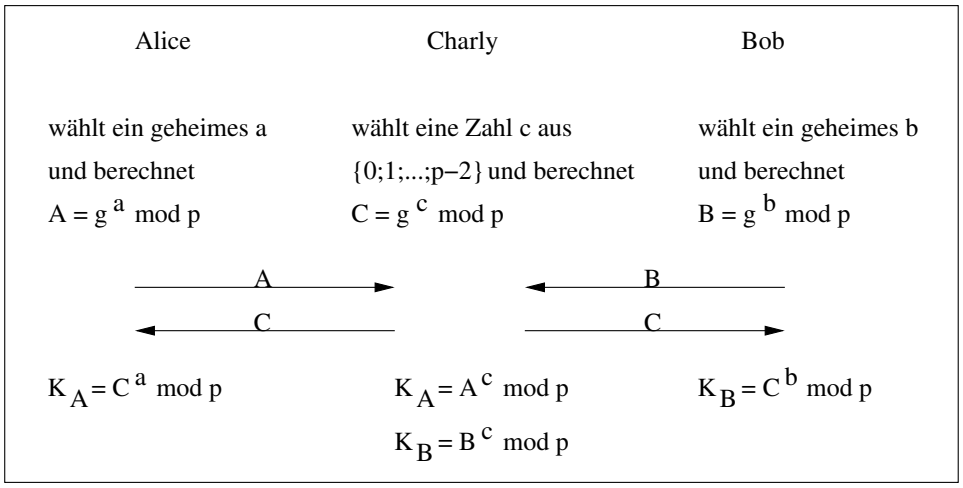


Abbildung 6.53: Man–in–the–Middle Angriff

Wegen

$$K_A = C^a \bmod p = g^{ac} \bmod p = A^c \bmod p \quad \text{und}$$
$$K_B = C^b \bmod p = g^{bc} \bmod p = B^c \bmod p$$

besitzt Charly sowohl einen gemeinsamen Schlüssel mit Alice, als auch einen mit Bob. Charly kann somit sämtliche Nachrichten zwischen Alice und Bob entschlüsseln und verändern, bevor er diese wieder mit dem jeweiligen Schlüssel des Empfängers chiffriert und weiterleitet.

Schutz vor diesem Angriff stellen die Verfahren zur Überprüfung der Authentizität von Nachrichten und Kommunikationspartnern (siehe Seite 127) dar.

6.3.4 RSA–Chiffrierung

Wie im Kapitel 6.3.2 gezeigt wurde, stellt die Produktbildung großer Primzahlen eine Einweg–Funktion dar[36)]. Auf dieser Eigenschaft beruht das RSA–Verfahren, das bekannteste Chiffrierverfahren der Public–Key–Kryptographie.

Neben der RSA–Chiffrierung ist die ElGamal–Verschlüsselung ein weiteres Verfahren asymmetrischer Verschlüsselung. In dieser Arbeit wird die unterrichtliche Behandlung des RSA–Verfahrens vorgeschlagen, da dieses im Vergleich zur ElGamal–Verschlüsselung folgende Vorteile aufweist:

- Das RSA–Verfahren ist die erste und bekannteste Verschlüsselungsmethode im Bereich der Public–Key–Kryptographie.
- Die Sicherheit des RSA–Verfahrens beruht auf dem Faktorisierungsproblem großer Zahlen. Die Schüler lernen dadurch eine praktische Anwendung dieser Problematik kennen.

[36)] siehe Seite 106

Die ElGamal–Verschlüsselung beruht auf dem Diffie–Hellman–Problem und bietet damit nichts Neues.

- Das RSA–Verfahren bietet durch Chiffrieren mit dem geheimen Schlüssel eine einfache Möglichkeit für elektronische Signaturen. Da im ElGamal–Chiffrierverfahren die Ver- und Entschlüsselung nicht einfach vertauscht werden können, ist die Erzeugung digitaler Signaturen in diesem Kryptosystem aufwändiger. Aus diesem Grund wird das RSA–Chiffrierverfahren auch im Hinblick auf das Kapitel "Nachrichtenauthentizität" bevorzugt.

Intentionen

- Die Schüler sollen in der Lage sein, Schlüssel für die RSA–Chiffrierung zu erzeugen.
- Die Schüler sollen die RSA–Chiffrierung durchführen können.
- Die Schüler sollen RSA–chiffrierte Texte bei Kenntnis des Schlüssels dechiffrieren können.
- Die Schüler sollen die Sicherheit der RSA–Verschlüsselung richtig beurteilen können.
- Die Schüler sollen Möglichkeiten zum Auffinden großer Primzahlen beschreiben können.

Inhalte
Bevor mit der Schlüsselerzeugung zur RSA–Chiffrierung begonnen werden kann, sind zunächst die Eulersche ϕ–Funktion, der euklidische Algorithmus sowie grundlegende Sätze zum größten gemeinsamen Teiler einzuführen.

Die Eulersche ϕ–Funktion
Für eine natürliche Zahl n definiert die Eulersche ϕ–Funktion

$$n \to \phi(n)$$

die Anzahl der zu n teilerfremden natürlichen Zahlen, die kleiner als n sind.

Beispielsweise sind die zur Zahl 12 teilerfremden Zahlen $\{1; 5; 7; 11\}$, womit $\phi(12) = 4$ gilt. Die Zahlen $\{1; 2; 3; 4; 5; 6\}$ sind teilerfremd zur Zahl 7, so dass $\phi(7) = 6$ ist.

Allgemein sind zu einer Primzahl p alle Zahlen von 1 bis $p-1$ teilerfremd. Folglich gilt für alle Primzahlen p

$$\phi(p) = p - 1.$$

Seien nun p und q zwei verschiedene Primzahlen. Dann gilt

$$\phi(pq) = (p-1)(q-1). \tag{6.6}$$

Beweis:
Insgesamt sind $pq - 1$ natürliche Zahlen kleiner als pq. Da p und q Primzahlen sind, sind unter diesen lediglich alle Vielfachen von p und alle Vielfachen zu q nicht teilerfremd zu pq.

Die Vielfachen von p, die kleiner als pq sind, sind die $q - 1$ Zahlen

$$\{p; 2p; 3p; ...; (q-1)p\};$$

die Vielfachen von q, die kleiner als pq sind, sind die $p-1$ Zahlen

$$\{q; 2q; 3q; ...; (p-1)q\}.$$

Die Anzahl der zu pq teilerfremden Zahlen erhält man nun, indem man von allen $pq-1$ Zahlen, die kleiner als pq sind, die Anzahl der oben ermittelten Vielfachen von p und q subtrahiert. Damit erhält man

$$\phi(pq) = (pq-1) - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1),$$

womit (6.6) bewiesen ist.

Der euklidische Algorithmus
Der euklidische Algorithmus ist ein Verfahren, um den größten gemeinsamen Teiler (ggT) zweier natürlicher Zahlen a und b ($a > b$) zu bestimmen.

Der Algorithmus beginnt, indem $a = r_0$ und $b = r_1$ gesetzt wird und anschließend die Division mit Rest in folgendem Verfahren angewandt wird.

$$\begin{aligned}
r_0 &= q_1 \cdot r_1 + r_2 && \text{mit } 0 < r_2 < r_1 \\
r_1 &= q_2 \cdot r_2 + r_3 && \text{mit } 0 < r_3 < r_2 \\
&... \\
r_i &= q_{i+1} \cdot r_{i+1} + r_{i+2} && \text{mit } 0 < r_{i+2} < r_{i+1} \\
&... \\
r_{n-3} &= q_{n-2} \cdot r_{n-2} + r_{n-1} && \text{mit } 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= q_{n-1} \cdot r_{n-1} + r_n && \text{mit } 0 < r_n < r_{n-1} \\
r_{n-1} &= q_n \cdot r_n
\end{aligned}$$

Das Verfahren bricht ab, wenn der Rest Null wird. Die Zahl r_n ist dann der größte gemeinsame Teiler von a und b.

Im Unterricht ist dieses Verfahren zunächst an einem Beispiel zu veranschaulichen. Seien beispielsweise $a = 2247$ und $b = 945$ zwei Zahlen, deren größter gemeinsamer Teiler bestimmt werden soll. Mit nachfolgendem Verfahren

$$\begin{aligned}
2247 &= 2 \cdot 945 + 357 \\
945 &= 2 \cdot 357 + 231 \\
357 &= 1 \cdot 231 + 126 \\
231 &= 1 \cdot 126 + 105 \\
126 &= 1 \cdot 105 + 21 \\
105 &= 5 \cdot 21
\end{aligned}$$

erhält man: ggT$(2247,945) = 21$.

Durch Probedivisionen überzeugt man sich bei Beispielen sehr leicht von der Richtigkeit der Behauptung, dass ggT(a,b) = r_n gilt. Anhand von Plausibilitätsüberlegungen ist diese Vermutung im Unterricht auch für den allgemeinen Fall zu belegen.

Hierzu überzeugt man sich, dass

1. r_n ein Teiler von a und b und dass
2. r_n der größte aller gemeinsamen Teiler von a und b

ist.

Um die erste Behauptung zu belegen, ist das euklidische Verfahren von unten nach oben zu durchlaufen. Wegen

$$r_{n-1} = q_n \cdot r_n$$

ist r_n ein Teiler von r_{n-1}. Mit

$$\begin{aligned} r_{n-2} &= q_{n-1} \cdot r_{n-1} + r_n \\ &= q_{n-1} \cdot q_n \cdot r_n + r_n \\ &= (q_{n-1} \cdot q_n + 1) \cdot r_n \end{aligned}$$

ist r_n aber auch ein Teiler von r_{n-2}. Wegen

$$\begin{aligned} r_{n-3} &= q_{n-2} \cdot r_{n-2} + r_{n-1} \\ &= q_{n-2} \cdot (q_{n-1} \cdot q_n + 1) \cdot r_n + q_n \cdot r_n \end{aligned}$$

ist r_n auch ein Teiler von r_{n-3}. Diese Argumentation wird fortgesetzt, bis man schließlich erkennt, dass r_n auch ein Teiler von r_1 und r_0, d. h. von a und b ist.

Um die zweite Behauptung zu zeigen, ist der euklidische Algorithmus von oben nach unten zu durchlaufen. Zu zeigen ist, dass jede Zahl z, mit $z|a$ und $z|b$ auch ein Teiler von r_n ist.

Sei z eine natürliche Zahl, mit $z|r_0$ und $z|r_1$. Dann gibt es ganze Zahlen k_0 und k_1 derart, dass gilt:

$$\begin{aligned} r_0 &= k_0 \cdot z \text{ und} \\ r_1 &= k_1 \cdot z. \end{aligned}$$

Wegen

$$\begin{aligned} & r_0 = q_1 \cdot r_1 + r_2 \\ \Leftrightarrow \quad & r_2 = r_0 - q_1 \cdot r_1 = k_0 z - q_1 k_1 z = (k_0 - q_1 k_1) \cdot z \end{aligned}$$

ist z auch ein Teiler von r_2. Damit gibt es eine ganze Zahl k_2, so dass $r_2 = k_2 \cdot z$ gilt. Dann ist mit

$$\begin{aligned} & r_1 = q_2 \cdot r_2 + r_3 \\ \Leftrightarrow \quad & r_3 = r_1 - q_2 \cdot r_2 = k_1 z - q_2 k_2 z = (k_1 - q_2 k_2) \cdot z \end{aligned}$$

z auch ein Teiler von r_3. Auf analoge Weise schließt man, dass z ein Teiler von $r_4, ..., r_{n-1}$ und schließlich auch von r_n ist.

Größter gemeinsamer Teiler
Mit Hilfe des euklidischen Algorithmus kann folgender Satz der Zahlentheorie gezeigt werden:

Seien a und b zwei natürliche Zahlen. Dann gibt es ganze Zahlen x und y mit

$$\text{ggT}(a,b) = xa + yb. \tag{6.7}$$

Beweis:
Die Behauptung erschließt sich, indem man den euklidischen Algorithmus von unten nach oben durchläuft und schrittweise die Reste wie folgt ersetzt:

$$\begin{aligned}
\text{ggT}(a,b) = r_n &= r_{n-2} - q_{n-1} \cdot r_{n-1} \\
&= r_{n-2} - q_{n-1} \cdot (r_{n-3} - q_{n-2} \cdot r_{n-2}) \\
&= (-q_{n-1}) \cdot r_{n-3} + (1 + q_{n-1} \cdot q_{n-2}) \cdot r_{n-2} \\
&= ... \\
&= (....)r_0 + (...)r_1.
\end{aligned}$$

Man kann folglich die Reste r_n, r_{n-1}, r_{n-2},... so lange ersetzten, bis nur noch r_0 und r_1 übrig bleiben. Die Werte in den Klammern sind dabei ganze Zahlen, womit die Behauptung gezeigt ist. Dieses Auflösen der Gleichungskette nach r_n wird auch als "erweiterter euklidischer Algorithmus" bezeichnet.

Seien z. B. $a = 23$ und $b = 8$ zwei Zahlen mit $\text{ggT}(23, 8) = 1$. Mit dem euklidischen Algorithmus

$$\begin{aligned}
23 &= 2 \cdot 8 + 7 \\
8 &= 1 \cdot 7 + 1 \\
7 &= 7 \cdot 1
\end{aligned}$$

erhält man auf folgende Weise

$$\begin{aligned}
1 &= 8 - 1 \cdot 7 \\
&= 8 - 1 \cdot (23 - 2 \cdot 8) \\
&= (-1) \cdot 23 + 3 \cdot 8
\end{aligned}$$

zwei ganze Zahlen, die die Gleichung (6.7) erfüllen.

Unter Anwendung von (6.7) kann wiederum nachfolgender Satz gezeigt werden, der für das RSA–Chiffrierverfahren von zentraler Bedeutung ist.

Sind a und b zwei teilerfremde Zahlen, dann gibt es eine ganze Zahl z, so dass gilt

$$z \cdot b \equiv 1 \bmod a. \tag{6.8}$$

Beweis:
Da a und b teilerfremd sind, ist der größte gemeinsame Teiler von a und b die Zahl 1. Nach (6.7) gibt es daher ganze Zahlen x und y welche die Gleichung

$$1 = xa + yb$$

erfüllen. Da

$$1 = xa + yb \Leftrightarrow xa = 1 - yb$$

gilt, ist a ein Teiler von $1 - yb$. Unter Anwendung der Äquivalenz (6.1) auf Seite 104 gilt damit:

$$yb \equiv 1 \bmod a.$$

Mit $y = z$ folgt die Behauptung (6.8).

Schlüsselerzeugung
Um ein Schlüsselpaar für das RSA–Chiffrierverfahren zu erzeugen, wählt man zufällig zwei geheim zu haltende Primzahlen p, q und berechnet

$$n = p \cdot q.$$

Anschließend bestimmt man $\phi(n)$ unter Anwendung von Satz (6.6) wie folgt

$$\phi(n) = (p - 1) \cdot (q - 1).$$

Zusätzlich wird eine zu $\phi(n)$ teilerfremde natürliche Zahl e mit $1 < e < \phi(n)$ gewählt und eine natürliche Zahl d mit $1 < d < \phi(n)$ berechnet, so dass gilt:

$$d \cdot e \equiv 1 \bmod \phi(n). \tag{6.9}$$

Da e und $\phi(n)$ teilerfremd sind, gibt es nach (6.8) die Zahl d tatsächlich. Diese Zahl d wird als Entschlüsselungsexponent bezeichnet und entspricht dem geheimen privaten Schlüssel eines Teilnehmers. Die Zahl n heißt RSA–Modul; e ist der Verschlüsselungsexponent. Die beiden Zahlen n und e stellen das öffentlich bekannte Schlüsselpaar eines Teilnehmers dar.

Im Unterricht ist die Schlüsselerzeugung an einem einfachen Beispiel zu veranschaulichen:

Seien $p = 13$ und $q = 7$ die gewählten geheimen Primzahlen. Dann ist

$$\begin{aligned} n &= 13 \cdot 7 = 91 \text{ und} \\ \phi(n) &= 12 \cdot 6 = 72. \end{aligned}$$

Um eine zu 72 teilerfremde Zahl zu finden, wendet man auf die Zahl 72 die Primfaktorzerlegung an und erhält: $72 = 2^3 \cdot 3^2$. Nun wählt man als Verschlüsselungsexponenten e z. B. die Zahl 5 und berechnet den euklidischen Algorithmus für die Zahlen 72 und 5 wie folgt:

$$\begin{aligned} 72 &= 14 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1. \end{aligned}$$

Der erweiterte euklidische Algorithmus hierzu

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (72 - 14 \cdot 5) \\ &= 29 \cdot 5 - 2 \cdot 72 \end{aligned}$$

liefert schließlich für den Entschlüsselungsexponenten d die Zahl 29, da offensichtlich

$$29 \cdot 5 \equiv 1 \bmod 72$$

gilt.

Verschlüsselung
Zur Verschlüsselung nach dem RSA–Verfahren sucht man sich aus einem Schlüsselverzeichnis zunächst den öffentlichen Schlüssel, bestehend aus den Zahlen n und e, heraus. Anschließend sind die Buchstaben – wie auf den Seiten 93ff gezeigt – als Zahlen darzustellen. Nun ist der Klartext in Blöcke m mit $0 \leq m < n$ einzuteilen.

Der Klartext m wird zum Kryptogramm c durch

$$c \equiv m^e \bmod n$$

verschlüsselt.

Seien z. B. wie im obigen Beispiel $n = 91$ und $e = 5$. Zu verschlüsseln sei der Buchstabe A. In ASCII wird A durch die Zahl 65 codiert. Das RSA–Verfahren chiffriert die Zahl 65 zu

$$65^5 \bmod 91 \equiv 39.$$

Entschlüsselung
Zur Entschlüsselung wendet man auf das Kryptogramm c die Berechnung

$$c^d \bmod n$$

an.

Im obigen Beispiel ergibt sich mit dem Entschlüsselungsexponenten $d = 29$ und der Rechnung

$$39^{29} \bmod 91 \equiv 65$$

die verschlüsselte Zahl 65 und damit der Klartextbuchstabe A.

Der Beweis von $m \equiv c^d \bmod n$ beruht auf dem kleinen Satz von Fermat. Da dieser Satz im Unterricht eingeführt und bewiesen werden müsste, erscheint im Rahmen eines Wahlunterrichts der Beweis von $m \equiv c^d \bmod n$ als zu aufwändig. Hier soll der Nachweis anhand von ausgewählten Beispielen genügen.

Sicherheit des RSA–Verfahrens
Die Sicherheit des RSA–Verfahrens hängt davon ab, dass aus dem öffentlichen Schlüssel – bestehend aus den Zahlen n und e – der geheime Schlüssel d nicht zu bestimmen ist. Wie im Abschnitt “Schlüsselerzeugung” gezeigt, ist d mit

$$d \cdot e \equiv 1 \bmod \phi(n)$$

über den erweiterten euklidischen Algorithmus zu berechnen. Dies bedeutet, dass die Sicherheit des RSA–Verfahrens von der Schwierigkeit abhängt, bei Kenntnis von n die Zahl $\phi(n)$ zu ermitteln.

Wegen $\phi(n) = (p-1) \cdot (q-1)$, benötigt man zur Berechnung von $\phi(n)$ die Zahlen p und q, womit obiges Problem auf die Faktorisierung von $n = p \cdot q$ zurückzuführen ist.

Im Kapitel "Einweg–Funktionen mit Falltüre" wurde gezeigt, dass die Faktorisierung großer Zahlen praktisch nicht durchführbar ist. Dazu sollte das RSA–Modul n mindestens 512 Bits, bei längerfristiger Geheimhaltung 1024 Bits (entspricht 309 Dezimalstellen) oder 2048 Bits (entspricht 617 Dezimalstellen) lang sein. Die Primzahlen p und q sollten dabei möglichst gleich groß und zufällig gewählt werden.

Die Schwierigkeit der Faktorisierung großer Primzahlprodukte lässt sich im Unterricht auch an publizierten Erfolgen über die Zerlegung großer Zahlen in ihre Primfaktoren veranschaulichen. Der hierzu erforderliche Aufwand zeigt deutlich, dass die Leistungsfähigkeit der Computer und die angewandten Verfahren zur Faktorisierung noch keine Gefahr für die Sicherheit des RSA–Verfahrens darstellen:

- Im Jahr 1994 gelang es D. Atkins, M. Graff, A. Lenstra und P. Leyland eine 129–stellige Dezimalzahl in 8 Monaten mithilfe von ca. 600 Mitarbeitern zu faktorisieren.
- Im Jahr 2005 erreichten F. Bahr, M. Boehm, J. Franke und T. Kleinjung von der Universität Bonn die Faktorisierung einer 200–stelligen Dezimalzahl. Die Faktorisierung hierzu begann Ende 2003 und dauerte bis Mai 2005, wobei insgesamt 80 Rechner zum Einsatz kamen[37)].

Um die Faktorisierung des RSA–Moduls möglichst schwer zu gestalten, ist darauf zu achten, dass die Primzahlen p und q nicht zu nahe beieinander liegen. Ist z. B. p nur geringfügig größer als q, kann folgendes Verfahren – auch als Faktorisierungsmethode von Fermat bezeichnet – schnell zum Erfolg führen:

Es sei a die kleinste ganze Zahl, die größer oder gleich $\sqrt{n}$ ist. Diese Zahl a wird schrittweise um 1 erhöht, bis $a^2 - n$ eine Quadratzahl b^2 ist. Dann gilt mit der 3. Binomischen Formel:

$$\begin{aligned} & a^2 - n = b^2 \\ \Rightarrow \quad & n = a^2 - b^2 = (a+b) \cdot (a-b) \\ \Rightarrow \quad & p = a + b \text{ und } q = a - b. \end{aligned}$$

Primzahlerzeugung

Wie im vorhergehenden Kapitel gezeigt, beruht die Sicherheit des RSA–Verfahrens im Wesentlichen auf der Produktbildung möglichst großer Primzahlen. Dass es unendlich viele Primzahlen gibt, hat bereits der griechische Mathematiker Euklid (365 – 300 v. Chr.) bewiesen. Im Unterricht ist in diesem Zusammenhang zu klären, wie Primzahlen überhaupt gefunden werden können. Für den Schulunterricht eignen sich diesbezüglich folgende Methoden:

- Das älteste Verfahren zum Auffinden von Primzahlen ist Schülern bereits aus dem Mathematikunterricht der Unterstufe unter dem Namen "Sieb des Eratosthenes" bekannt.

[37)] vgl. http://www.rsa.com/rsalabs/node.asp?id=2879
Um die Sicherheit des RSA–Verfahrens zu überprüfen, veröffentlicht die Vertreiberfirma Zahlen, für deren Faktorisierung Preisgelder ausgesetzt werden.

Hierbei werden alle Zahlen von 1 bis zu einer bestimmten, frei wählbaren Zahl x aufgeschrieben. Beginnend bei der Zahl 2 wird diese als Primzahl notiert und alle Vielfachen von 2 weggestrichen. Im nächsten Schritt wird die Zahl 3 als Primzahl aufgeschrieben und alle Vielfachen der 3 werden gestrichen. Die nächste noch nicht durchgestrichene Zahl ist 5, die als Primzahl notiert wird, bevor alle Vielfachen von 5 gestrichen werden. Man fährt auf diese Weise fort und erhält alle Primzahlen von 1 bis zur gewählten Zahl x.

- Eine weitere klassische Methode zur Erzeugung von Primzahlen stammt vom schweizer Mathematiker Leonhard Euler (1707 – 1783). Er gab die Formeln

$$n^2 + n + 17 \quad \text{und}$$
$$n^2 + n + 41$$

an, die für natürliche Zahlen n mit $0 < n < 16$ bzw. $0 < n < 40$ Primzahlen liefern.

- Nach dem französischen Mönch und Mathematiker Marin Mersenne (1588 – 1648) sind Zahlen der Form

$$2^p - 1$$

benannt. Ist p eine Primzahl, befinden sich unter diesen Zahlen besonders viele Primzahlen. Zum Beispiel sind die Mersenne–Zahlen $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$ usw. Primzahlen. Dass aber nicht alle Mersenne–Zahlen Primzahlen sind, zeigt sich bereits für $p = 11$, da $2^{11} - 1 = 2047 = 23 \cdot 89$ gilt.

- Die vom französichen Mathematiker und Jurist Pierre de Fermat (1607 – 1665) stammenden Fermat–Zahlen der Form

$$2^{2^n} + 1$$

sind für $n = 0, 1, 2, 3, 4$ ebenfalls Primzahlen. Entgegen seiner Vermutung, dass alle weiteren Zahlen dieser Form Primzahlen seien, zeigte bereits 1732 Euler, dass für $n = 5$ das Produkt $641 \cdot 6700417$ gilt.

Zusammenfassend kann festgehalten werden, dass es kein Verfahren zur Erzeugung von Primzahlen gibt. Ein – für Schüler ausreichendes – praktisches Vorgehen zum Auffinden von Primzahlen ist mit dem Computeralgebrasystem SAGE möglich[38)]. Der Befehl "next_prime (x)" gibt zu einer zufällig gewählten Zahl x die kleinste Primzahl $> x$ an. Zu beachten ist allerdings, dass solche Funktionen in der Regel auf Primzahltests beruhen, die nur mit großer Wahrscheinlichkeit Primzahlen liefern.

Will man eine bereits gegebene Zahl n daraufhin überprüfen, ob diese eine Primzahl ist, besteht die Möglichkeit der Probedivision. Hierzu wird n durch probeweises Dividieren auf Teilbarkeit zu allen Primzahlen von 1 bis $\sqrt{n}$ getestet. Befindet sich unter diesen kein Teiler, ist n eine Primzahl.

[38)] siehe Seite 107

6.3.5 PGP–Chiffrierung

Wie bereits zu Beginn dieses Kapitels angesprochen, erfordern asymmetrische Chiffrierverfahren erheblich mehr Rechenleistung als symmetrische Verschlüsselungen. Da es auch sichere symmetrische Chiffrierverfahren gibt, wird in der Praxis bevorzugt symmetrisch verschlüsselt. Asymmetrische Verfahren werden in diesem Zusammenhang für den Austausch der hierzu benötigten Schlüssel herangezogen. Damit werden die Vorteile beider Chiffrierverfahren genutzt: geringer Rechenaufwand und unkomplizierter Schlüsselaustausch auch über unsichere Kanäle. Dieses Vorgehen wird als "hybride Verschlüsselung" bezeichnet.

Das – nicht zuletzt wegen seiner Entstehungsgeschichte – bekannteste hybride Verschlüsselungsprogramm ist das von Phil Zimmermann entwickelte und 1991 veröffentlichte Verfahren "Pretty Good Privacy", kurz PGP genannt.

Für die Behandlung von PGP im Unterricht sprechen folgende Gründe:

- Der Einsatz von PGP ist aus motivationalen Gründen sinnvoll. Schüler können anhand einer frei verfügbaren und damit kostenlosen Verschlüsselungssoftware das theoretisch erlangte Wissen über asymmetrische Kryptosysteme praktisch anwenden.
- Die Entstehungsgeschichte von PGP ist ein Musterbeispiel dafür, wie unterschiedlich die Meinungen über die private Anwendung kryptographischer Methoden ausfallen können. Je nach Sichtweise können Vor- als auch Nachteile der Kryptographie erarbeitet werden.
- Die Rolle der US Justiz bei der Verbreitung von PGP eröffnet die Möglichkeit, die Haltung der Bundesregierung zur Kryptologie und die Rechtmäßigkeit ihrer Anwendung zu überprüfen.
- Das PGP–Verfahren bietet die Möglichkeit, Texte elektronisch zu signieren und Unterschriften zu überprüfen. Damit stellt PGP eine praktische Anwendungsmöglichkeit im Kapitel über Authentizität dar.

Intentionen

- Die Schüler sollen die Funktionsweise hybrider Verschlüsselungssoftware beschreiben können.
- Die Schüler sollen in der Lage sein, PGP zu installieren und verantwortungsbewusst zu nutzen.

Inhalte
PGP ist ein von Phil Zimmermann entwickeltes E–Mail–Verschlüsselungsprogramm für den privaten Gebrauch, das als hybrides Chiffrierverfahren arbeitet. Da eine asymmetrische Verschlüsselung einer ganzen Nachricht zu rechenintensiv wäre, wird die eigentliche Nachricht symmetrisch und nur der hierzu benötigte Schlüssel asymmetrisch chiffriert. Dazu wird für jede Verschlüsselung ein neuer Sitzungsschlüssel generiert, mit dem öffentlichen Schlüssel des Empfängers im RSA- bzw. ElGamal–Kryptosystem chiffriert und der verschlüsselten Nachricht hinzugefügt.

Beim Empfänger entschlüsselt PGP mit dessen privaten Schlüssel des asymmetrischen Kryptosystems zunächst den symmetrischen Schlüssel und dechiffriert mit diesem anschließend das erhaltene Kryptogramm.

Entstehungsgeschichte von PGP
Die Idee hinter der Entwicklung von PGP war, dass das Versenden chiffrierter E–Mails für jede Person möglich sein sollte. Als Menschenrechtsvertreter und Friedensaktivist war das Ziel des Erfinders Phil Zimmermann, die Privatsphäre gegenüber staatlichen Behörden zu schützen.

Nach Fertigstellung der ersten Version von PGP, wurde diese 1991 zur kostenlosen Nutzung im Internet veröffentlicht, kurz nachdem in den USA das Gesetz zur "Zusammenarbeit zwischen Telekommunikationsherstellern und der Regierung" erlassen wurde. Dieses verpflichtete alle Anbieter von Kommunikationsgeräten auf Verlangen den Klartext der Daten staatlichen Behörden vorzulegen. Mit der Veröffentlichung von PGP wurde die Möglichkeit zur Offenlegung des Klartextes stark eingeschränkt und Phil Zimmermann wurde zum Ziel der amerikanischen Justiz.

Diese vertrat die Auffassung, dass Zimmermann durch die Verbreitung von PGP über die USA hinaus gegen die Exportbestimmungen des Landes verstoßen hatte. Verschlüsselungssoftware zählt in den USA zu den Rüstungsgütern und hätte nur mit Genehmigung des Außenministeriums verbreitet werden dürfen. Nach jahrelangen Untersuchungen wurde das Verfahren gegen ihn 1996 eingestellt.

Die Anklageerhebung gegen Zimmermann entfesselte eine weltweite Debatte darüber, wie weit Verschlüsselung den Bürgern zugänglich und legal nutzbar gemacht werden dürfte. Dass Verschlüsselung notwendig ist, um Daten großer Unternehmen über ihre Produkte und Kunden oder Daten beim elektronischen Einkauf über das Internet vor unerlaubten Zugriffen zu schützen, ist sofort ersichtlich. Aber die private Nutzung kryptographischer Methoden bietet sowohl Vorteile als auch Nachteile, die an dieser Stelle auch im Unterricht diskutiert bzw. anhand eines Rollenspiels zwischen Menschenrechtsvertretern und Ermittlungsbehörden herausgearbeitet werden sollten. Um die Kritik- und Urteilsfähigkeit der Schüler zu fördern, sollten vor allem folgende Argumente Eingang in den Unterricht finden:

Argumente gegen einen privaten Gebrauch von Verschlüsselungsmethoden:

- Kryptographie schützt nicht nur die elektronische Kommunikation gesetzestreuer Bürger, sondern auch die von Kriminellen und Terroristen. Abhöraktionen der Strafverfolger können bei verschlüsselter Kommunikation keine Verbrecher mehr überführen.
- Die Möglichkeit, elektronischen Schriftverkehr zu verschlüsseln, unterstützt auch das weltweite organisierte Verbrechen. Die Vorhaben werden nicht mehr telefonisch abgesprochen, sondern über gesicherte Übertragungen durch das Internet.
- Kriminelle bewahren Pläne durch verschlüsseltes Abspeichern sicher auf. Dadurch wird das Auffinden von Beweisen und damit die Überführung der Verbrecher erheblich erschwert.
- Abhörsysteme wie z. B. das von USA, England, Kanada, Australien und Neuseeland betriebene Spionagenetz "Echelon" überprüft den Nachrichtenverkehr auf bestimmte be-

denkliche Stichwörter. Der Gebrauch von Verschlüsselungen macht dieses System wertlos, worin die USA eine Gefahr für die nationale Sicherheit sieht.

Argumente für einen privaten Gebrauch von Verschlüsselungsmethoden:

- Verschlüsselung steht im Einklang mit Artikel 12 der Allgemeinen Erklärung der Menschenrechte: "Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, sein Heim oder seinen Briefwechsel noch Angriffen auf seine Ehre und seinen Beruf ausgesetzt werden. Jeder Mensch hat Anspruch auf rechtlichen Schutz gegen derartige Eingriffe oder Anschläge."
- Kryptographie schützt die Privatsphäre von Bürgern gegenüber ungerechtfertigten Abhöraktionen. Systeme wie das oben beschriebene "Echelon" beschränken sich nicht auf einzelne Personenkreise und können den Nachrichtenverkehr von jedem Bürger überprüfen.
- Die z. B. über Abhöraktionen erhaltenen Daten können missbraucht werden. Dies ist sowohl im Bereich der Wirtschaftsspionage als auch bei erhaltenen Daten über politische Gegner möglich[39)].

Lösungsansätze, die die Interessen beider Lager in Einklang bringen sollten, war z. B. die Schlüsselhinterlegung bei staatlichen Behörden. Aufgrund fehlendem Vertrauen in staatliche Instanzen konnte sich dieser Ansatz nicht durchsetzen.

An dieser Stelle sollte im Unterricht die deutsche Rechtslage im Hinblick auf die Nutzung kryptographischer Methoden angesprochen werden. Wie beim Bundesministerium des Innern nachzulesen ist, hat die Bundesregierung am 02. Juni 1999 Eckpunkte der deutschen Kryptopolitik beschlossen, die bis heute Gültigkeit haben. Im ersten Eckpunkt wird insbesondere folgendes versichert:

"Die Bundesregierung beabsichtigt nicht, die freie Verfügbarkeit von Verschlüsselungsprodukten in Deutschland einzuschränken. Sie sieht in der Anwendung sicherer Verschlüsselung eine entscheidende Voraussetzung für den Datenschutz der Bürger, für die Entwicklung des elektronischen Geschäftsverkehrs sowie für den Schutz von Unternehmensgeheimnissen. Die Bundesregierung wird deshalb die Verbreitung sicherer Verschlüsselung in Deutschland aktiv unterstützen. Dazu zählt insbesondere die Förderung des Sicherheitsbewußtseins bei den Bürgern, der Wirtschaft und der Verwaltung"[40)].

Entsprechend dieser Vorgabe hat die Bundesregierung 1999 die Weiterentwicklung von PGP durch den Düsseldorfer Programmierer Werner Koch zu GNU Privacy Guard[41)] finanziell unterstützt.

Praktische Anwendung von PGP

Da ausführliche Installationsbeschreibungen von PGP in [12] und auf zahlreichen Internetseiten erhältlich sind, wird in dieser Arbeit nicht weiter darauf eingegangen. Wie bereits zu Beginn

[39)] vgl. [30], S. 365ff

[40)] Nachzulesen unter http://www.bmi.bund.de

[41)] GNU Privacy Guard ist ein frei erhältliches E–Mail–Verschlüsselungsprogramm auf der Grundlage von PGP.

dieses Kapitels angesprochen, ist PGP ein hybrides Verschlüsselungsverfahren. Entsprechend weist diese Software folgende Funktionen auf:

- PGP generiert Paare von öffentlichen und privaten Schlüsseln für das RSA– bzw. ElGamal–Kryptosystem.
- PGP erzeugt zufällige Sitzungsschlüssel, mit denen der Text einer E–Mail verschlüsselt wird.
- PGP chiffriert den Sitzungsschlüssel mit dem öffentlichen Schlüssel des Empfängers und fügt diesen der E–Mail an.
- PGP dechiffriert den Sitzungsschlüssel beim Empfänger mit dem privaten Schlüssel und entschlüsselt das erhaltene Kryptogramm.

Wichtig ist an dieser Stelle, dass die Schüler nach der Installation die Verschlüsselung ausprobieren, indem sie ihre öffentlichen Schlüssel austauschen und sich gegenseitig verschlüsselte E–Mails schicken. Da PGP das Generieren eines Sitzungsschlüssels und dessen Chiffrierung mit dem öffentlichen Schlüssel automatisch ausführt, werden die zu Beginn des Kapitels 6.3 vorgestellten Schritte der asymmetrischen Verschlüsselung nochmals vor Augen geführt.

Außerdem sollten Schüler darauf hingewiesen werden, dass die gesamte Sicherheit von PGP auf einer Passphrase[42)] beruht, die bei der Installation einzugeben ist. Mit dieser Passphrase wird der private Schlüssel vor dem Abspeichern chiffriert. Hier sollten Kriterien für das Auffinden einer “sicheren” Passphrase angegeben werden, wie z. B. die Verwendung eines langen Satzes mit Zahlen oder Sonderzeichen, der dennoch für den Anwender leicht zu merken ist.

Neben den oben genannten Funktionen bietet PGP auch die Möglichkeit, Dateien elektronisch zu signieren und PGP–chiffrierte Unterschriften zu überprüfen. Auf diese Möglichkeiten wird im nachfolgenden Kapitel eingegangen.

6.3.6 Zusammenfassung

In diesem Kapitel wird zunächst die Funktionsweise asymmetrischer Kryptosysteme im Vergleich zu symmetrischen Chiffrierverfahren dargestellt. Da für asymmetrische Chiffrierverfahren die Modulo–Rechnung von zentraler Bedeutung ist, wird anschließend die Modulo–Rechnung eingeführt und später benötigte Rechenregeln bewiesen.

Da asymmetrische Chiffrierverfahren auf Einweg–Funktionen mit Falltüre beruhen, wird im darauffolgenden Kapitel die Einweg–Eigenschaft der Produktbildung großer Primzahlen experimentell nachgewiesen und die Einweg–Eigenschaft der diskreten Exponentialfunktion anhand des Rechenaufwands von Beispielen plausibel gemacht.

Als erster Algorithmus der Public–Key–Kryptographie gilt der Diffie–Hellman–Schlüsselaustausch, dessen Funktionalität unter Einbeziehung der Einweg–Eigenschaft der diskreten Expo-

[42)] Eine Passphrase ist eine beliebige Wort- und Zeichenfolge.

nentialfunktion bewiesen wird. Überlegungen zur Sicherheit dieses Verfahrens schließen das Kapitel ab.

Mit dem RSA–Verfahren wird das bedeutendste Verfahren der Public–Key–Kryptographie behandelt. Hierzu sind mit der Eulerschen ϕ–Funktion, dem euklidischen Algorithmus und Eigenschaften des größten gemeinsamen Teilers zunächst ausgewählte Inhalte der Zahlentheorie einzuführen. Nachdem die Ver- und Entschlüsselung beim RSA–Verfahren anhand von Beispielen demonstriert und geübt wurde, werden Überlegungen zur Sicherheit sowie zum Auffinden großer Primzahlen angestellt.

Als praktische Anwendungsmöglichkeit asymmetrischer Verschlüsselungen wird das E–Mail–Verschlüsselungsprogramm PGP vorgestellt und diese frei verfügbarer Software am PC installiert. Die Entstehungsgeschichte von PGP eignet sich besonders, um auf unterschiedliche Sichtweisen über den privaten Gebrauch kryptographischer Methoden sowie auf die Kryptopolitik der Bundesregierung einzugehen.

6.4 Authentizität und Integrität

Im bisherigen Unterricht ging es vor allem darum, Nachrichten für eine außenstehende Person unleserlich zu machen. Man spricht in diesem Fall auch von Schutz gegen einen passiven Angriff. Einhergehend mit den Zielen der Kryptologie (siehe Seite 51) werden in heutiger Zeit kryptographische Methoden verstärkt gegen aktive Angriffe eingesetzt. Das beinhaltet Forderungen nach

- Nachrichtenintegrität: Sicherstellung, dass die Nachricht nicht durch unbefugte Dritte verändert wurde;
- Nachrichtenauthentizität: Sicherstellung, dass die Nachricht wirklich vom angegebenen Absender stammt;
- Benutzerauthentikation: Sicherstellung, dass der Kommunikationspartner wirklich die Person ist, für die er sich ausgibt.

6.4.1 Nachrichtenintegrität

Die Überprüfung der Integrität einer Nachricht ist mit Hashfunktionen möglich. Nach der Definition von Hashfunktionen sind neben kryptographischen Anforderungen auch Möglichkeiten zur Konstruktion von Hashfunktionen im Unterricht zu behandeln.

Intentionen

- Die Schüler sollen die Eigenschaften kryptographischer Hashfunktionen nennen können.
- Die Schüler sollen eine Möglichkeit zur Konstruktion kryptographischer Hashfunktionen beschreiben können.

Inhalte
Da die Grenzen zwischen Nachrichtenintegrität und Nachrichtenauthentizität fließend sind, sollte in dieses Kapitel mit einem typischen Beispiel für die Integrität von Daten eingeführt werden.

Methoden zur Überprüfung der Integrität von Daten werden z. B. eingesetzt, wenn jemand an einem Programm oder einem Dokument arbeitet und sicherstellen möchte, dass während seiner Abwesenheit niemand daran unerlaubte Änderungen angebracht hat. Hierzu wird aus dem Programm bzw. dem Dokument mit kryptographischen Verfahren ein bestimmter Prüfwert ermittelt. Nach der Abwesenheit des Benutzers wiederholt dieser das Verfahren und überprüft, ob der erhaltene Wert mit dem zuvor ermittelten Prüfwert übereinstimmt. Ist dies nicht der Fall, wurde am erstellten Programm bzw. Dokument manipuliert.

Kryptographische Verfahren, mit denen man einen Prüfwert ermitteln kann, basieren auf Hashfunktionen.

Kryptographische Hashfunktionen
Allgemein wird mit einer Hashfunktion h eine Nachricht m von beliebiger Länge auf einen Wert $h(m)$ fester Länge abgebildet.

Liegt eine Nachricht im binären ASCII–Code vor, so ist z. B. die duale Addition der einzelnen Ziffern ohne Übertrag eine Hashfunktion. Das Ergebnis ist 1, falls die Anzahl der Einsen in m ungerade ist, andernfalls 0.

Man überzeugt sich leicht, dass zu obigem Beispiel einer Hashfunktion mehrere unterschiedliche Nachrichten mit dem gleichen Hashwert gefunden werden können. Zudem zeigt das Beispiel auch, dass Hashfunktionen nicht injektiv sind.

Da auf diese Weise die Integrität von Daten nicht garantiert werden kann, werden an die in der Kryptographie angewandten Hashfunktionen weitere Anforderungen gestellt:

- Kryptographische Hashfunktionen sollen die Einweg–Eigenschaft aufweisen:
  - Zu einer gegebenen Nachricht m kann der Hashwert $h(m)$ effizient berechnet werden.
  - Aus dem gegebenen Hashwert $h(m)$ soll es praktisch unmöglich sein, m zu berechnen.
- Es ist praktisch unmöglich, zu einer vorgegebenen Nachricht m eine Nachricht m' zu finden, mit $h(m) = h(m')$. Funktionen mit dieser Eigenschaft werden auch als schwach kollisionsresistent bezeichnet.

Häufig wird in kryptographischen Anwendungen gefordert, dass die Hashfunktion (stark) kollisionsresistent ist. In diesem Fall ist es praktisch unmöglich, irgendwelche Nachrichten m und m' zu finden, die denselben Hashwert haben. Diese Anforderung wird vor allem an die im nächsten Kapitel erläuterten elektronischen Signaturen gestellt.

Im Unterricht sollte an dieser Stelle ein Beispiel zur Konstruktion einer kryptographischen Hashfunktion zur Überprüfung der Nachrichtenintegrität vorgestellt werden.

Konstruktion von Hashfunktionen
Eine Möglichkeit zur Berechnung einer Prüfsumme ist die Anwendung eines symmetrischen Verschlüsselungsalgorithmus im Cipher–Block–Chaining–Modus. Die Prüfsumme ergibt sich dabei nach folgendem Verfahren:

1. Zunächst wird ein (binärer) Text m in Blöcke $m_1, m_2, ..., m_k$ gleicher Länge eingeteilt. Ein eventuell unvollständiger letzter Block m_k wird mit Füllbits auf die gewünschte Länge gebracht.

2. Nun wendet man eine Verschlüsselungsfunktion f auf den ersten Block an und erhält $c_1 = f(m_1)$.

3. Bevor die Verschlüsselungsfunktion auf den zweiten Block m_2 angewandt wird, wird c_1 zu m_2 ohne Übertrag addiert. Man erhält folglich $c_2 = f(m_2 \oplus c_1)$.

4. Auf analoge Weise erhält man als Ergebnis des dritten Blocks $c_3 = f(m_3 \oplus c_2)$. Allgemein gilt $c_i = f(m_i \oplus c_{i-1})$ für alle weiteren Blöcke des Klartextes.

5. Das Kryptogramm des letzten Blocks $c_k = f(m_k \oplus c_{k-1})$ wird als kryptographische Prüfsumme herangezogen.

Dieses Vorgehen hat den Vorteil, dass die Prüfsumme unabhängig von der Länge der Nachricht immer dieselbe Länge aufweist und dass sie von der gesamten Nachricht abhängt und nicht nur von einem Teil.

Das MD5–Verfahren
Die genaue Analyse der Funktionsweise der in der Praxis angewandten kryptographischen Hashfunktionen wie z. B. SHA-1 (Secure Hash Algorithm) oder MD5 (Message Digest Algorithm 5) erscheint für den Schulunterricht zu komplex. Da jedoch die im folgenden Kapitel zu behandelnde PGP–Signatur auf dem Hashwert von MD5 basiert, ist an dieser Stelle der Einsatz entsprechender Software zur Berechnung von MD5–Hashwerten sinnvoll. Positiv ist auch, dass durch eine Analyse der Ergebnisse, die Eigenschaften von Hashfunktionen nochmals vor Augen geführt werden.

Hashwerte von MD5	
a	0cc175b9c0f1b6a831c399e269772661
Geheimnis	cfed27322417affc616b3bfbc2a9faa2
Hashberechnung ohne alle Geheimniskrämerei	388f601037c9e293c17340ff5f619943
Hashberechnung ohne alle Geheimniskrämerei.	4c7bcc5bd2a458b27e8ab0d15aa92865
Hashberechnung ohne alle Geheimniskrämerei .	cfc7fe405f1753eabd28d6cba0495dce
Hashberechnung ohne alle Geheimniskrämerei!	bb9f013259b4a4b1655ecc46576ddac4

Wie obige Tabelle deutlich macht, erzeugt MD5 aus einem Text beliebiger Länge – auch wenn er nur aus einem Buchstaben besteht – eine 128 Bit lange Zahl, die als 32 Zeichen lange Hexadezimalzahl dargestellt wird. Kleine Änderungen im Text wie z. B. an Satzzeichen oder zusätzliche Leerzeichen führen zu völlig anderen Werten.

Allgemein ist festzuhalten, dass man mit Hilfe von Hashfunktionen feststellen kann, ob Daten verändert wurden oder nicht. Man kann aber nicht überprüfen, von wem die Nachricht stammt. Die Überprüfung der Authentizität einer Nachricht wird im folgenden Kapitel erläutert.

6.4.2 Nachrichtenauthentizität

Intentionen

- Die Schüler sollen die Notwendigkeit der Nachrichtenauthentizität an Beispielen belegen können.
- Die Schüler sollen das Verfahren zur Überprüfung der Authentizität einer Nachricht mithilfe des Message Authentication Codes beschreiben können.
- Die Schüler sollen in der Lage sein, digitale Signaturen zu berechnen und zu verifizieren.
- Die Schüler sollen Möglichkeiten der elektronischen Unterschrift verantwortungsbewusst nutzen können.

Inhalte
Die Methoden zur Überprüfung der Nachrichtenauthentizität beruhen auf der Annahme, dass nur der Urheber einer Nachricht über einen geheimen Schlüssel s verfügt. Dabei kann die Urheberschaft einer Nachricht auf grundsätzlich zwei verschiedene Weisen erbracht werden: mit dem Message Authentication Code oder mit einer digitalen Unterschrift.

Die Überprüfung der Nachrichtenauthentizität aufgrund eines Schlüssels kann im Unterricht mit einem gläsernen Tresor veranschaulicht werden (vgl. Abbildung 6.54). Jeder kann die Nachricht im gläsernen Tresor lesen, aber nur der Eigentümer des Tresors kann eine Nachricht in diesen hinterlegen. Deshalb wird davon ausgegangen, dass jede Nachricht im Tresor von dessem Eigentümer stammt[43)].

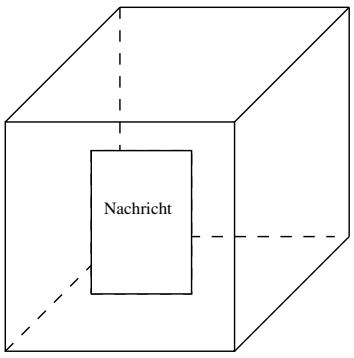


Abbildung 6.54: Der gläserne Tresor

[43)] vgl. [9], Seite 17

6.4.2.1 Message Authentication Code

Zur Einführung in dieses Thema ist Schülern die Notwendigkeit der Nachrichtenauthentizität bewusst zu machen. Die Anwendung des Message Authentication Codes wird an folgendem Beispiel besonders deutlich:

Eine Professorin Alice sendet per E-Mail an das Prüfungsamt eine Liste mit den Martrikelnummern derjenigen Studenten, die eine Prüfung erfolgreich bestanden haben. Diese Liste muss nicht geheim gehalten werden. Im Gegenteil, sie wird im Schaukasten öffentlich ausgehängt. Das Prüfungsamt muss dagegen sicher sein, dass die Liste tatsächlich von Alice stammt und nicht von einem findigen Studenten abgeschickt wurde. Die Nachrichtenauthentizität kann in diesem Fall mit dem Message Authentication Code gewährleistet werden[44)].

Die Nachrichtenauthentizität mit dem Message Authentication Code – kurz als MAC bezeichnet – ist ein Verfahren, das innerhalb eines beschränkten Personenkreises durchführbar ist. Hierzu wird der MAC einer Nachricht m mithilfe einer kryptographischen Hashfunktion h_s generiert, die von einem Parameter s abhängt[45)]. Der Wert des Parameters entspricht dem geheimen Schlüssel und ist zuvor zwischen den Kommunikationspartnern auf einem sicheren Weg auszutauschen.

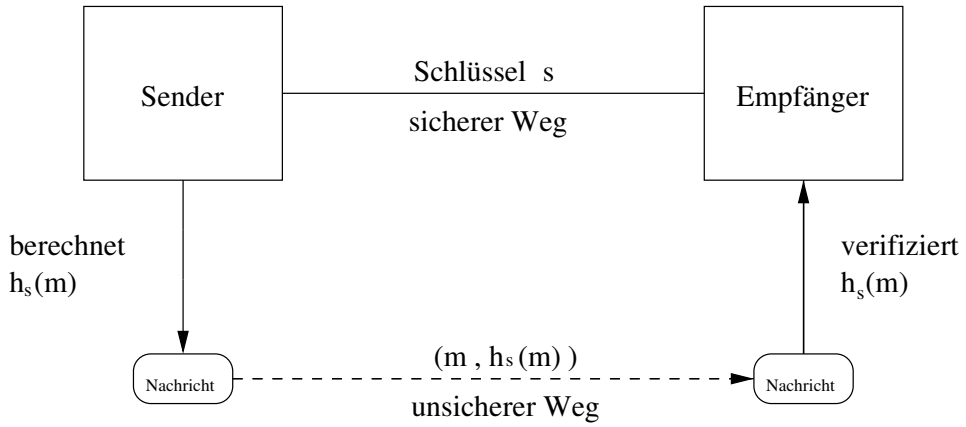


Abbildung 6.55: Nachrichtenauthentizität mit Message Authentication Codes

Wie in Abbildung 6.55 dargestellt, trifft beim Empfänger neben der Nachricht m' der MAC $h_s(m)$ ein. Der Empfänger berechnet nun $h_s(m')$ und überprüft die Übereinstimmung mit $h_s(m)$. Sind die Werte gleich, wird die Nachricht als authentisch akzeptiert.

Das häufigste Verfahren zur Berechnung des MAC ist ein symmetrisches Chiffrierverfahren im Cipher–Block–Chaining–Modus auf Grundlage eines gemeinsamen Schlüssels. Das Vorgehen erfolgt analog zur Berechnung einer Prüfsumme zum Nachweis der Nachrichtenintegrität (vgl. oben). Der MAC entspricht dabei dem Kryptogramm des letzten Blocks einer Nachricht.

[44)] vgl. [10], Seite 201

[45)] Die Hashfunktion verfügt über dieselben Eigenschaften wie auf Seite 128 dargelegt.

Das Verfahren des Message Authentication Codes hat den Nachteil, dass zwischen den Kommunikationspartnern auf einem sicheren Weg ein Schlüssel ausgetauscht werden muss, weshalb dieses Vorgehen vor allem innerhalb eines eng begrenzten Personenkreises Anwendung findet. Aus diesem Grund haben sich in der Praxis digitale Signaturen zur Überprüfung der Nachrichtenauthentizität durchgesetzt.

6.4.2.2 Digitale Signaturen

Digitale Signaturen werden in Public–Key–Kryptosystemen ermöglicht und bieten neben der Überprüfung der Nachrichtenauthentizität den Vorteil, dass die Signatur nicht abgestritten werden kann. Aufgrund dieser Verbindlichkeit werden elektronische Signaturen bei vielen Kaufverträgen im Internet oder bei verbindlichen E–Mails vorgenommen.

Da das RSA– und das PGP– Chiffrierverfahren bereits im Kapitel "Asymmetrische Kryptosysteme" behandelt wurden, ist die unterrichtliche Behandlung von digitalen Signaturen innerhalb dieser Public–Key–Kryptosysteme vorgesehen.

RSA–Signaturen

Die Schlüsselerzeugung für RSA–Signaturen erfolgt analog zur Schlüsselerzeugung für RSA–Chiffrierverfahren[46)]. Man wählt zufällig zwei geheim zu haltende Primzahlen p und q und berechnet die beiden Werte

$$\begin{aligned} n &= p \cdot q \\ \phi(n) &= (p-1) \cdot (q-1). \end{aligned}$$

Anschließend wird eine zu $\phi(n)$ teilerfremde natürliche Zahl e mit $1 < e < \phi(n)$ gewählt und eine natürliche Zahl d mit $1 < d < \phi(n)$ berechnet, so dass

$$d \cdot e \equiv 1 \bmod \phi(n)$$

gilt.

Das öffentliche Schlüsselpaar ist (n,e) und d ist der geheime Schlüssel des Teilnehmers.

Erzeugung der Signatur
Bevor mit der Signatur einer Nachricht gestartet werden kann, ist die Nachricht analog zur RSA–Verschlüsselung als Zahlenfolge darzustellen und in Blöcke m mit $0 \leq m < n$ einzuteilen.

Signiert wird ein Zahlenblock m durch s mit

$$s \equiv m^d \bmod n.$$

Zu beachten ist, dass die RSA–Signatur auf gleiche Weise wie ein Kryptogramm erzeugt wird, mit dem Unterschied, dass der Nachrichtenblock bei der Signatur mit dem geheimen privaten Schlüssel potenziert wird. Insofern stellt s die RSA–Entschlüsselung von m dar.

[46)] siehe Seite 119

Aufgrund der Einschränkung der Nachricht auf eine bestimmte Größe, können mit diesem Verfahren lediglich kurze Nachrichten signiert werden. In der Praxis wird dieser Mangel dadurch behoben, dass eine Nachricht zunächst mittels einer Hashfunktion auf eine Zahl kleiner n abgebildet wird und nur der Hashwert signiert wird.

Verifikation der Signatur
Angenommen Alice schickt eine Nachricht m zusammen mit der Signatur s an Bob. Dieser sucht aus einem Schlüsselverzeichnis das öffentliche Schlüsselpaar (n,e) heraus und überprüft, ob

$$m \equiv s^e \bmod n$$

gilt. Stimmen die Werte überein, weiß Bob, dass die Nachricht m tatsächlich von Alice stammt, da nur sie den geheimen Schlüssel d kennt. Die Signatur ist nämlich die RSA–Entschlüsselung von m, die nur mit dem privaten Schlüssel d möglich ist.

Im Unterricht ist an dieser Stelle das RSA–Signierverfahren an einem Beispiel zu veranschaulichen:

Seien wie im Kapitel "Asymmetrische Chiffrierverfahren" (auf Seite 119) $p = 13$ und $q = 7$. Man berechnet $n = 91$ sowie $\phi(n) = 72$ und erhält mit $e = 5$ den privaten Schlüssel $d = 29$. Soll die Nachricht $m = 71$ signiert werden, berechnet Alice

$$71^{29} \bmod 91 \equiv 15$$

und schickt das Paar (m,s) mit $(71,15)$ an Bob. Dieser berechnet mit dem öffentlichen Schlüsselpaar (n,e)

$$15^5 \bmod 91 \equiv 71.$$

Da dieser Wert mit der Nachricht $m = 71$ übereinstimmt, wird die Nachricht als authentisch von Alice akzeptiert.

PGP–Signaturen

Wie bereits im Kapitel "Asymmetrische Chiffrierverfahren" dargelegt, sollen die Lernenden anhand von PGP eine praktische Anwendung digitaler Signaturen kennen lernen. Denn Schüler verspüren Freude, theoretisch erlangtes Wissen in die Praxis umzusetzen, wodurch sie für weitere Lernziele motiviert sind und die Behaltensleistung wesentlich gefördert wird. Durch den Einsatz entsprechender Software können Schüler auch zum verantwortungsbewussten Umgang mit Signaturverfahren angeleitet werden.

PGP bietet dem Anwender die Möglichkeit, Dateien automatisch zu signieren. Hierzu wird nach Erstellen der Nachricht intern der MD5–Hashwert des ASCII–Codes des Textes berechnet. Anschließend wird der MD5–Wert mit dem privaten Schlüssel des Anwenders chiffriert und an die Nachricht angehängt.

Um die Signatur einer erhaltenen Nachricht mittels PGP zu überprüfen, geht das Programm wie folgt vor:

- Der MD5–Hashwert des ASCII–Codes der Nachricht wird erneut berechnet.

- Mit dem öffentlichen Schlüssel wird die mitgeschickte digitale Unterschrift dechiffriert. Man erhält den MD5–Hashwert des Absenders.
- Beide MD5–Werte werden miteinander verglichen. Stimmen Sie überein, gilt die Nachricht als authentisch.

Im Unterricht ist das Signieren mit PGP auszuprobieren, indem sich die Schüler gegenseitig signierte E–Mails verschicken. Hierbei erkennen sie, dass

- Nachrichten sowohl als Klartext wie auch als Kryptogramm mit einer elektronischen Unterschrift verschickt werden können und dass
- durch die digitale Signatur neben Authentizität einer Nachricht auch die Integrität überprüft werden kann. Denn eine Veränderung des Textes führt zu einer Veränderung des MD5–Hashwertes und damit zu einer anderen Signatur.

Sicherheit digitaler Signaturen

Nach der Darlegung der Funktionsweise elektronischer Signaturen, ist im Unterricht die praktische Bedeutung zu erörtern. Die beschriebenen Verfahren haben eine gemeinsame Schwachstelle darin, dass die elektronische Signatur mit einem privaten geheimen Schlüssel vorgenommen wird. Dies beinhaltet zwei Gefahren:

- Bob könnte ein öffentliches Schlüsselpaar generieren und unter dem Namen von Alice veröffentlichen. Nun kann Bob alle Nachrichten im Namen von Alice versenden und signieren.
- Alice signiert eine Nachricht mit ihrem privaten Schlüssel. Später behauptet sie, dass die Signatur nicht von ihr stammt.

Sollen digitale Signaturen praktische Anwendung erlangen, muss folglich sichergestellt werden, dass der öffentliche Schlüssel authentisch ist, d. h. dem tatsächlichen Eigentümer gehört. Diese Forderung beinhaltet auch, dass durch elektronische Signaturen der Urheber einer Nachricht nachweislich identifiziert werden kann.

Bei der praktischen Beseitigung der beschriebenen Schwachstelle ist zwischen regulierten und nicht regulierten Verfahren zu unterscheiden. Zu den nicht regulierten Verfahren gehören z. B. PGP–Signaturen.

Regulierte Verfahren

Rechtsgrundlage für das Angebot von elektronischen Signaturen stellt das “Gesetz über Rahmenbedingungen für elektronische Signaturen” vom 16. Mai 2001 dar. Das kurz als Signaturgesetz (SigG) bezeichnete Gesetz hat nach §1 zum Ziel, “Rahmenbedingungen für elektronische Signaturen zu schaffen” und damit ein gewisses Maß an Rechtssicherheit zu gewährleisten.

Zur Rechtssicherheit gehört auch, die Authentizität öffentlicher Schlüssel zu gewährleisten. Hierzu sind vom Gesetzgeber Zertifizierungsdiensteanbieter vorgesehen, die

- für eine Person ein Schlüsselpaar, bestehend aus einem privaten Signaturschlüssel und einem öffentlichen Signaturprüfschlüssel zur Verifikation der Signatur erzeugen und

- für diese Person ein Zertifikat ausstellen, mit dem bestätigt wird, dass ein bestimmtes Signaturschlüsselpaar dieser Person zugeordnet wurde.

Da alle Zertifizierungsdiensteanbieter bei der Bundesnetzagentur anzuzeigen sind, kann somit jeder über diese Agentur die Gültigkeit einer elektronischen Signatur nachprüfen. Ein solches System, das es ermöglicht, Zertifikate für öffentliche Schlüssel auszustellen und zu überprüfen, wird als "Public–Key–Infrastuktur", kurz PKI bezeichnet.

Im Unterricht ist in diesem Zusammenhang das Signaturgesetz einzusetzen und insbesondere folgende Inhalte zu erarbeiten:

- Obwohl nach §1 SigG die Verwendung elektronischer Signaturen grundsätzlich freigestellt ist, unterscheidet §2 SigG "elektronische Signaturen", "fortgeschrittene elektronische Signaturen" und "qualifizierte elektronische Signaturen".
- Die "qualifizierten elektronischen Signaturen" erfüllen die Anforderungen des Signaturgesetzes und basieren auf einem gültigen qualifizierten Zertifikat. Das Signaturgesetz bestimmt in §7 die Anforderungen an diese qualifizierten Zertifikate und in §4 die Anforderungen an die Zertifizierungsdiensteanbieter, die diese Zertifikate ausstellen.
- Zertifizierungsdiensteanbieter müssen bei der Bundesnetzagentur angezeigt werden. Im Internet ist unter http://www.bundesnetzagentur.de eine Liste von Zertifizierungsdiensteanbietern veröffentlicht.

Nach Inkrafttreten des Signaturgesetztes wurden Gesetzesänderungen beschlossen. So wurde z. B. §126 BGB dahingehend ergänzt, dass (mit Ausnahmen) die "gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden" kann. In diesem Fall ist das "elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz" zu versehen.

Web of Trust

Ein zum hierarchisch angeordneten System des PKI entgegengesetztes Verfahren, die Authentizität öffentlicher Schlüssel zu überprüfen, ist das "Netz des Vertrauens" bzw. das "Web of Trust". Die Aufgabe der Bundesnetzagentur wird hier von allen Teilnehmern durch gegenseitige Bestätigungen übernommen. Das Public–Key–Kryptosystem PGP bzw. das freie GnuPG basieren auf diesem Verfahren.

Hierzu wird jeder Schlüssel in einer PGP–Schlüsseldatei mit zwei Parametern versehen:

- Validität: ein Gradmesser für die Überzeugung, dass ein öffentlicher Schlüssel der angegebenen Person gehört.
- Vertrauen: ein Gradmesser für das Vertrauen, das man der Person entgegenbringt, die einen Schlüssel generiert hat.

Grundgedanke dieses Systems ist, dass, wenn man von der Validität eines Schlüssels überzeugt ist und dieser Person ein hohes Maß an Vertrauen entgegenbringt, auch von der Validität der Schlüssel überzeugt ist, die diese Person signiert hat. Vereinfacht kann dies auf folgende Schlussfolgerung zurückgeführt werden: vertraut Charly Bob und signiert Bob den öffentlichen Schlüssel von Alice, dann akzeptiert Charly diesen Schlüssel von Alice als authentisch.

Ein wichtiger Indikator für die Validität eines Schlüssels ist der Fingerabdruck, der auch als Fingerprint bezeichnet wird. Der Fingerprint ist der MD5–Hashwert des öffentlichen PGP–Schlüssels.

Nach dieser Einführung ist im Unterricht der Schlüsselaustausch im Web of Trust beispielhaft aufzuzeigen.

- Alice generiert ein PGP–Schlüsselpaar und stellt ihren öffentlichen Schlüssel in ein Schlüsselverzeichnis wie z. B. einem Schlüsselserver.
- Bob möchte an Alice eine vertrauliche Nachricht schicken und diese deshalb mit dem öffentlichen Schlüssel von Alice verschlüsseln. Hierzu sucht Bob aus dem Schlüsselverzeichnis den öffentlichen PGP–Schlüssel von Alice heraus.
- Um sicher zu sein, dass der angegebene Schlüssel authentisch ist, d. h. tatsächlich Alice gehört, fragt Bob über einen sicheren Kanal Alice nach ihrem Fingerprint.
- Nun vergleicht Bob den von Alice angegebenen Fingerprint mit dem MD5–Hashwert des aus dem Schlüsselverzeichnis herausgesuchten Schlüssels. Sind beide Werte gleich, ist Bob von der Authentizität des Schlüssels überzeugt.
- Bob signiert nun den öffentlichen Schlüssel von Alice mit seinem privaten Schlüssel und schickt diesen mitsamt der Signatur wieder an den öffentlichen Schlüsselserver zurück. Bobs Signatur stellt nun für diesen Schlüssel ein Zertifikat dar.
- Nun möchte Charly ebenfalls an Alice eine verschlüsselte Nachricht schicken und sucht deshalb den öffentlichen Schlüssel von Alice heraus. Dieser Schlüssel besitzt nun die Signatur von Bob. Damit weiß Charly, dass Bob bereits die Authentizität des Schlüssels überprüft hat. Wenn Charly Bobs öffentlichen Schlüssel schon hat und Bob vertraut, dass er den Schlüssel von Alice gründlich überprüft hat, dann akzeptiert Charly den herausgesuchten Schlüssel von Alice ebenfalls als authentisch und braucht nicht mehr bei Alice nachzufragen.

Im Unterricht sollte untersucht werden, inwiefern die Verschlüsselungssoftware PGP die Umsetzung des Web of Trust unterstützt. Die Lernenden sollten erkennen, dass PGP dieses Verfahren fördert, indem der Anwender vier mögliche Stufen des Vertrauens einem öffentlichen Schlüssel – und damit seinem Benutzer – zuordnen kann. Vom Grad des Vertrauens hängt ab, wie sich die Verschlüsselungssoftware PGP in Zukunft verhält:

- Bei nicht zertifizierten Schlüsseln fragt PGP immer nach, ob man diese selbst zertifizieren möchte. Hier ist die Überprüfung mit dem Fingerprint zu empfehlen.
- Bei Schlüsseln, die von Personen zertifiziert wurden, denen der Anwender nicht oder nur eingeschränkt vertraut, wird die Signatur mitgeteilt und es wird angeboten, den Schlüssel selbst zu zertifizieren.
- Bei Schlüsseln, die von Personen zertifiziert wurden, denen der Anwender uneingeschränkt vertraut, wird der Schlüssel sofort als authentisch akzeptiert.

Daneben bietet PGP die Möglichkeit, den Vertrauensgrad von öffentlichen Schlüsseln zu verändern oder (unbekannte) Signaturen vor dem Abspeichern auf dem Rechner zu entfernen.

6.4.3 Benutzerauthentizität

Nachdem im vorherigen Kapitel Verfahren zur Nachrichtenauthentizität aufgezeigt wurden, geht es jetzt um Methoden, die die Identität des Kommunikationspartners nachweisen. Hierzu gibt es drei grundlegende Möglichkeiten:

- Die Identität einer Person kann durch biologische Eigenschaften nachgewiesen werden. Dazu gehören z. B. der klassische und der genetische Fingerabdruck oder die Gesichtserkennung.
- Eine Person kann durch den Besitz eines einzigartigen Gegenstandes ihre Identität nachweisen. Dazu gehört z. B. der Personalausweis. Auch beim Bezahlen mit einer Geldkarte wird davon ausgegangen, dass der Karteninhaber der berechtigte Benutzer ist.
- Eine Person kann ihre Identität durch ihr Wissen nachweisen. Beim Homebanking ist z. B. die Eingabe einer persönlichen Identifikationsnummer notwendig, um auf sein Konto zugreifen zu können.

In der Kryptographie wird vor allem durch die letzte Methode die Identität eines Teilnehmers nachgewiesen. Lernziele hierzu sind:

- Die Schüler sollen die Notwendigkeit der Benutzerauthentizität anhand von Beispielen erläutern können.
- Die Schüler sollen das Verfahren der Identifikation anhand von Passwörtern erklären können.
- Die Schüler sollen in der Lage sein, das Passwortverfahren in der Praxis sicher anzuwenden.
- Die Schüler sollen das Verfahren der Challenge–and–Response–Identifikation erläutern können.
- Die Schüler sollen in der Lage sein, Zero–Kowledge–Verfahren durchzuführen.

6.4.3.1 Passwortverfahren

Die einfachste kryptographische Methode zur Sicherstellung der Benutzerauthentizität besteht im Passwortverfahren. Im Unterricht sollte dieses Thema anhand von Beispielen aus der Lebenswelt der Schüler eingeführt werden. Hierzu gehören z. B. folgende Anwendungen:

- Jeder Schüler der Schule hat die Berechtigung, die Computer der Schule zu nutzen. Dazu erhält jeder Schüler neben einer Benutzerkennung ein Passwort zugewiesen. Beim An-

melden an einem PC kann der Benutzer durch Angabe von Kennwort und Passwort seine Identität und damit seine Zugangsberechtigung nachweisen.

- Beim Abheben von Geld an einem Geldausgabeautomaten ist neben der Bank– bzw. EC–Karte die persönliche Identifikationsnummer (PIN) vonnöten. Neben der Authentifizierung des Benutzers durch seinen Besitz (Karte) wird hier die Sicherheit durch die zusätzliche Abfrage eines Passwortes (PIN) erhöht.
- Beim Homebanking erhält man durch Angabe seiner Benutzerkennung und der PIN Zugang zum Konto. Geldtransaktionen sind allerdings nur durch Angabe einer zusätzlichen Transaktionnummer (TAN) möglich. Da eine TAN nur einmal verwendet werden kann, stellt diese ein Einmal–Passwort dar.

Da Systemadministratoren Zugang zu Passwortdateien haben können, werden Passwörter auf Rechnern verschlüsselt abgespeichert. Hierzu wird in der Regel eine Einwegfunktion verwendet und nur der Funktionswert auf der Festplatte gesichert. Meldet sich der Benutzer an einem Rechner an, wird auf das eingegebene Passwort die Einwegfunktion angewandt und der Funktionswert mit dem in der Passwortdatei abgespeicherten Wert verglichen. Stimmen beide Werte überein, wird der Benutzer als authentisch akzeptiert.

Wie obige Beispiele zeigen, weisen Schüler bei zahlreichen Systemen ihre Identität mittels Passwörtern nach. Im Unterricht sollten deshalb Regeln für den Umgang mit Passwörtern aufgestellt werden. Neben dem Gebot, Passwörter anderen Personen nicht mitzuteilen oder aufzuschreiben, gehören dazu insbesondere folgende Hinweise:

- Passwörter sollten gelegentlich geändert werden. Je häufiger ein Passwort verwendet wird, desto höher ist die Gefahr, dass es z. B. durch unverschlüsselte Übertragung abgehört wurde.
- Die Übermittlung des Passwortes vom Benutzer zum System sollte sicher sein. So ermöglicht z. B. HTTPS[47)] eine verschlüsselte Datenübertragung über das Internet.
- Das Passwort sollte mindestens 6 Zeichen lang sein und neben Buchstaben auch Ziffern oder Sonderzeichen enthalten. Dadurch wird dem Wörterbuchangriff – bei dem ein Angreifer alle Wörter eines Wörterbuches durchprobiert – begegnet.

Ein Nachteil des Passwortverfahrens besteht darin, dass das Geheimnis über einen längeren Zeitraum gleich ist. Ein abgehörtes Passwort kann folglich zu einem späteren Zeitpunkt unbefugt verwendet werden. Diese Gefahr ist bei Challenge–and–Response–Verfahren verringert, da hier die übermittelten Daten zur Authentifizierung variiert werden.

6.4.3.2 Challenge–and–Response

Die grundlegende Idee der Challenge–and–Response–Verfahren besteht darin, eine unvorhersehbare Frage zu stellen, die der Kommunikationspartner mithilfe seines geheimen Wissens beantworten kann.

[47)] Hypertext Transfer Protocol Secure

Zur Überprüfung der Teilnehmerauthentizität müssen beide Kommunikationspartner eine Einwegfunktion, die von einem geheimen Schlüssel abhängt, kennen. Alternativ ist auch eine symmetrische Verschlüsselungsmethode auf Grundlage eines geheimen Schlüssels möglich. Wie in Abbildung 6.56 dargestellt, überprüft Alice die Identität von Bob in folgenden Schritten:

Challenge:
Alice wählt zufällig eine Zahl (RAND) und schickt diese an Bob.

Response:
Bob berechnet das Ergebnis der Einwegfunktion bzw. Verschlüsselungsfunktion f_k(RAND) = RES und sendet diese an Alice.

In der Zwischenzeit berechnet Alice ihrerseits f_k(RAND) und überprüft nun, ob ihr Ergebnis mit der Antwort von Bob übereinstimmt.

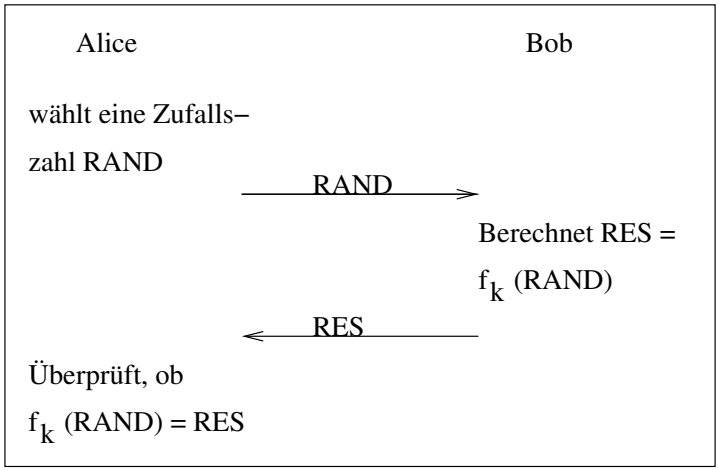


Abbildung 6.56: Challenge–and–Response mit symmetrischer Verschlüsselungsfunktion bzw. schlüsselabhängiger Einwegfunktion f_k

Im Unterricht ist dieses Verfahren mit bereits behandelten symmetrischen Verfahren wie z. B. der Vernam–Chiffrierung durchzuspielen. Hierzu einigen sich zwei Schüler auf einen genügend langen, geheim zu haltenden Schlüssel. Anschließend schickt ein Schüler (Verifizierer) dem anderen (Beweiser) eine zufällig gewählte Zahl. Zu dieser addiert der Beweiser den Schlüssel ohne Übertrag und schickt das Ergebnis dem Verifizierer zurück. Nach einmaliger Anwendung ist der Schlüssel neu zu vereinbaren.

Anstelle einer schlüsselabhängigen Einwegfunktion bzw. einer symmetrischen Verschlüsselungsfunktion sind Challenge–and–Response–Verfahren auch mit Signaturverfahren möglich. In diesem Fall schickt Alice eine Zufallszahl an Bob, der diese Zahl signiert und an Alice zurücksendet. Alice überprüft nun die signierte Zahl mit dem öffentlichen Schlüssel von Bob. Vorteil dieses Verfahrens ist, dass Alice den geheimen Schlüssel von Bob nicht kennt. Bei Verwendung von symmetrischen Verfahren oder Einwegfunktionen müssen beide Kommunikationspartner das Geheimnis besitzen.

Neben Challenge–and–Response–Verfahren auf Basis elektronischer Signaturen gibt es spezielle Verfahren, bei denen ein Teilnehmer jemanden davon überzeugen kann, ein bestimmtes Geheimnis zu besitzen, ohne dieses Geheimnis zu verraten. Solche Identifikationsverfahren werden als Zero–Knowledge–Verfahren bezeichnet und sind im Folgenden zu behandeln.

6.4.3.3 Zero–Knowledge–Verfahren

Zero–Knowledge–Verfahren sind dadurch gekennzeichnet, dass ein Beweiser ein Geheimnis kennt, der Verifizierer jedoch nicht. Während des Verfahrens überzeugt der Beweiser den Verifizierer davon, das Geheimnis zu kennen. Der Verifizierer erfährt während des Protokolls jedoch nicht das geringste über das Geheimnis.

Das bekannteste und wichtigste Zero–Knowledge–Verfahren ist das 1986 von Amos Fiat und Adi Shamir veröffentlichte Fiat–Shamir–Protokoll.

Schlüsselerzeugung
Der Beweiser Bob wählt analog zum RSA–Verfahren zwei geheim zu haltende Primzahlen p und q und berechnet eine öffentlich bekannt zu gebende Zahl n durch

$$n = p \cdot q.$$

Anschließend wählt Bob zufällig eine zu n teilerfremde Zahl s aus $\{1; ...; n-1\}$ und berechnet v mit

$$v \equiv s^2 \bmod n.$$

Die Zahl s ist das Geheimnis von Bob, während die Zahl v öffentlich bekannt gemacht wird. Folglich stellt das Paar (n, v) den öffentlichen Schlüssel von Bob dar.

Anstelle von Bob kann auch eine zentrale Schlüsselvergabestelle die entsprechenden Berechnungen durchführen, die Zahl s nur Bob mitteilen und das Schlüsselpaar (n, v) öffentlich bekannt geben.

Protokoll
Während des Protokolls überzeugt Bob, die Verifiziererin Alice, dass er das Geheimnis s kennt, ohne diese Zahl preis zu geben:

- Bob wählt zufällig eine Zahl r aus $\{1; 2; ...; n-1\}$, berechnet $x \equiv r^2 \bmod n$ und sendet den Wert x an Alice.
- Alice wählt zufällig eine Zahl $b \in \{0; 1\}$ und sendet diese an Bob.
- Bob berechnet y mit $y \equiv rs^b \bmod n$ d. h.
  - es gilt $y = r$ für $b = 0$,
  - und $y \equiv rs \bmod n$ für $b = 1$.

  Anschließend sendet er den Wert y an Alice.
- Alice verifiziert diese Antworten indem sie

- für $b = 0$ überprüft, ob $y^2 \bmod n \equiv x$ gilt und
- für $b = 1$ testet, ob $y^2 \bmod n \equiv xv \bmod n$ ist.

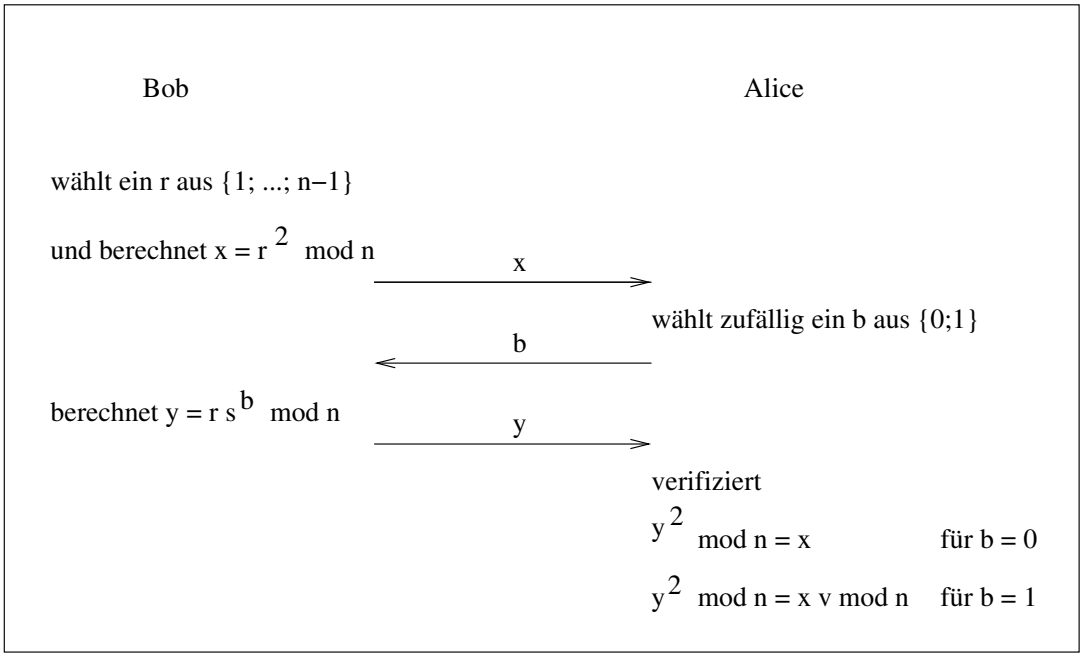


Abbildung 6.57: Fiat–Shamir–Protokoll

Durchführbarkeit
Im Unterricht ist die Durchführbarkeit des Protokolls zu beweisen. Hierzu zeigt man mithilfe der Rechenregeln auf Seite 104, dass

für $b = 0$

$$\begin{aligned} y^2 \bmod n &\equiv r^2 \bmod n \\ &\equiv x \end{aligned}$$

und für $b = 1$

$$\begin{aligned} y^2 \bmod n &\equiv (rs \bmod n)^2 \bmod n \\ &\equiv (r \bmod n \cdot s \bmod n)^2 \bmod n \\ &\equiv (r^2 \bmod n \cdot s^2 \bmod n) \bmod n \\ &\equiv (x \cdot v) \bmod n \end{aligned}$$

gilt.

Beispiel
Im Anschluss an die theoretischen Überlegungen ist im Unterricht ein konkretes Beispiel zu berechnen. Seinen hierzu $p = 3$ und $q = 17$, so erhält man $n = 3 \cdot 17 = 51$. Anschließend wählt man z. B. $s = 19$ und erhält $v \equiv 19^2 \bmod 51 \equiv 4$. Die möglichen Protokolle zeigen die Abbildungen 6.58 bzw. 6.59.

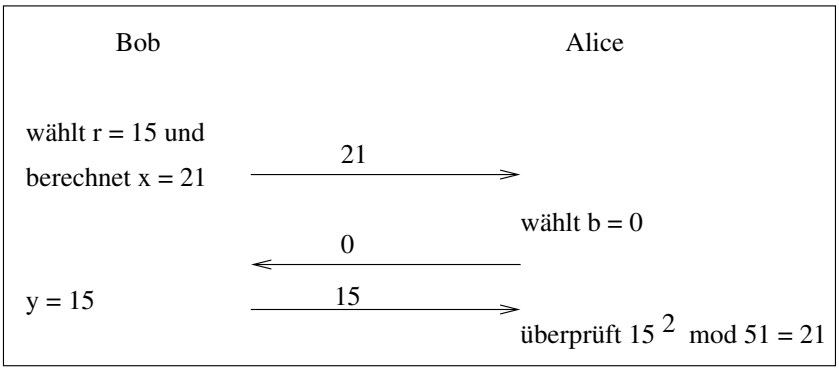


Abbildung 6.58: Beispiel eines Fiat–Shamir–Protokolls mit b = 0

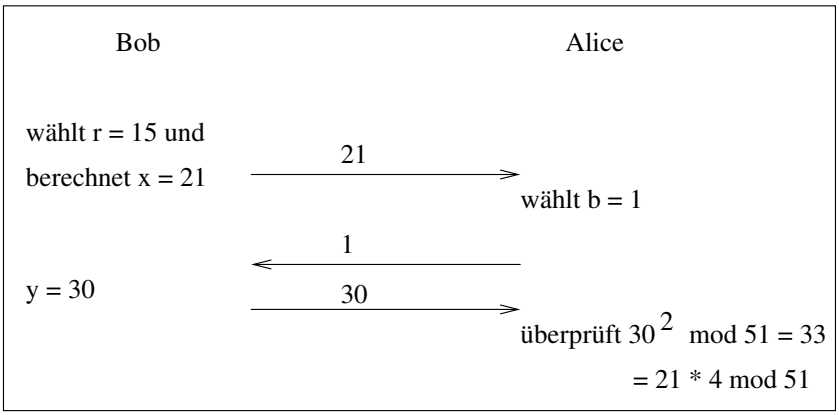


Abbildung 6.59: Beispiel eines Fiat–Shamir–Protokolls mit b = 1

Das Beispiel zeigt, dass Bob mit der Kenntnis der Quadratwurzel s von v mod n beide mögliche Fragen von Alice beantworten kann. Im Folgenden ist zu analysieren, ob sich jemand anderer (z. B. Charly) auch ohne Kenntnis von s als Bob ausgeben kann.

Sicherheit
Ohne Kenntnis von s kann Charly nicht beide Fragen beantworten. Er kann allerdings versuchen, die Zahl x so zu wählen, dass er eine der beiden möglichen Antworten richtig bestimmen kann.

Vermutet Charly, dass Alice $b = 0$ wählen wird, so wählt er $x = r^2$ mod n. Liegt er mit seiner Vermutung richtig, kann er an Alice die ihm bekannte Zahl r schicken. Liegt er dagegen falsch, kann er die Frage von Alice nicht beantworten.

Vermutet Charly, dass Alice $b = 1$ wählen wird, so wählt er zuerst ein y und bestimmt $x = y^2v^{-1}$ mod n. Liegt er mit seiner Vermutung richtig, so verifiziert Alice wegen

$$y^2 \text{ mod } n \equiv y^2v^{-1} \text{ mod } n \cdot v \text{ mod } n$$

auch diese Antwort als richtig. Allerdings kann er die Frage für $b = 0$ nicht beantworten.

Dies bedeutet, dass sich ein unberechtigter Dritter mit der Wahrscheinlichkeit $\frac{1}{2}$ als Bob identifizieren kann. Will Alice folglich sicher sein, dass Bob ihr Kommunikationspartner ist, ist das Protokoll wiederholt anzuwenden. Bei k erfolgreichen Durchführungen des Fiat–Shamir–Protokolls liegt die Wahrscheinlichkeit, mit einem unberechtigten Dritten zu kommunizieren bei $\frac{1}{2^k}$.

Zusammenfassend gilt, dass mithilfe des Fiat–Shamir–Protokolls die Authentizität eines Teilnehmers mit beliebig großer Sicherheit nachgewiesen werden kann, ohne dass der Verifizierer das Geheimnis des Kommunikationspartners kennt, oder das Geheimnis während des Protokolls herausfinden kann.

6.4.4 Zusammenfassung

In diesem Kapitel geht es um kryptographische Verfahren zur Gewährleistung von Authentizität und Integrität von Nachrichten sowie um Methoden der Identifikation von Personen.

Hierzu werden zunächst Hashfunktionen eingeführt und ihre Bedeutung für den Nachweis der Nachrichtenintegrität behandelt. Als Beispiel einer in der Praxis angewandten Hashfunktion dient das MD5–Verfahren, dessen Hashwerte analysiert werden.

Im Bereich der Nachrichtenauthentizität werden neben dem Message Authentication Code digitale Signaturen behandelt. Aufgrund des vorhandenen Vorwissens der asymmetrischen Chiffrierverfahren RSA und PGP werden die elektronischen Unterschriften dieser Kryptosysteme erläutert. Nach den Überlegungen zur Erzeugung und Verifikation digitaler Signaturen wird die Sicherheit dieser Verfahren kritisch reflektiert. Unter Einbeziehung des Signaturgesetzes lernen die Schüler mit der Public–Key–Infrastruktur und dem Web of Trust zwei grundsätzlich verschiedene Lösungsansätze zum Nachweis der Authentizität öffentlicher Schlüssel kennen.

Schließlich werden im Kapitel Benutzerauthentizität kryptographische Verfahren vorgestellt, mit denen die Identität von Personen nachgewiesen werden kann. Neben dem weit verbreiteten Passwortverfahren wird das Challenge–and–Response–Verfahren behandelt. Das Fiat–Shamir–Protokoll wird abschließend als Beispiel eines Zero–Knowledge–Verfahrens vorgestellt, bei denen ein Verifizierer keinerlei Hinweise auf das Geheimnis des Beweisers erhält und dennoch von der Kenntnis dieses Geheimnisses überzeugt wird.

7 Praxiserfahrungen

Die in dieser Arbeit vorgestellte Unterrichtssequenz wurde im Schuljahr 2006/2007 an der Städtischen Elly–Heuss–Realschule in München in einem Wahlunterricht Kryptologie durchgeführt. An dieser sechsstufigen Realschule werden die drei Wahlpflichtfächergruppen

I mit dem Schwerpunkt im mathematisch–naturwissenschaftlich–technischen Bereich,

II mit dem Schwerpunkt im wirtschaftlichen Bereich und

III mit dem Schwerpunkt im musisch–gestaltenden Bereich

angeboten. Das Schulprofil ist durch eine musisch–künstlerische Ausbildung geprägt, was sich in Bläserklassen, im Wahlunterricht Ballett, sowie jährlichen Theateraufführungen und Konzerten widerspiegelt.

Im Folgenden werden die Erfahrungen dargelegt, die im Rahmen des Wahlunterrichts Kryptologie gesammelt wurden.

7.1 Zusammensetzung der Lerngruppe

Entsprechend dem Kapitel “Didaktischer Ort eines Unterrichts in Kryptologie”, wurde der Wahlunterricht Kryptologie für Schülerinnen und Schüler der Jahrgangsstufen 9 und 10 angeboten. Teilgenommen haben zwei Schülerinnen und acht Schüler, die alle die 10. Jahrgangsstufe besuchten.

Wahlpflichtfächergruppen
Eine Aufteilung der Teilnehmer nach besuchten Wahlpflichtfächergruppen zeigt, dass Schüler des Ausbildungszweiges I deutlich überwiegen (vgl. Abbildung 7.1). Folglich ist das Interesse an Kryptologie bei Schülern mit mathematisch–naturwissenschaftlichen Neigungen besonders hoch.

Eine Befragung der Teilnehmer nach Ihrer Freizeitbeschäftigung stellte heraus, dass sich ca. 40% für Technik bzw. Elektrotechnik interessieren und ca. 30% viel Freizeit am Computer verbringen. Dies bestätigt obige Vermutung, dass sich vor allem mathematisch–technisch orientierte Jugendliche für Kryptologie interessieren.

Vorkenntnisse in Informatik
Der in dieser Arbeit vorgestellte Lehrplan in Kryptologie[1)] sieht Wahlpflichtbereiche vor, aus

[1)] siehe Seite 45ff

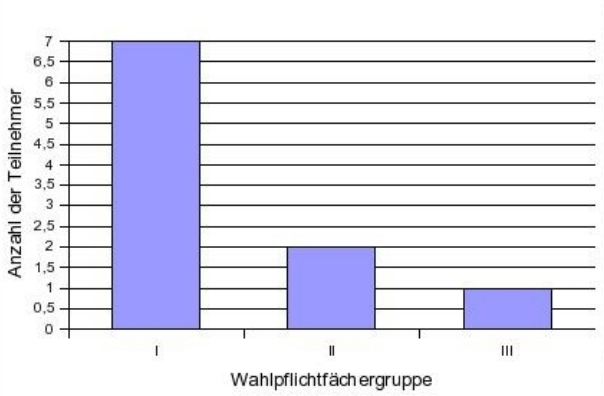


Abbildung 7.1: Teilnehmeranzahl nach Wahlpflichtfächergruppen I, II und III

denen jeweils ein Themengebiet auszuwählen ist. Diese Wahlpflichtbereiche beinhalten auch Lerninhalte, die Programmierkenntnisse erfordern. Da die am Wahlunterricht Kryptologie teilgenommenen Schüler keine vertieften Programmiererfahrungen besaßen, wurden jeweils die Wahlpflichtthemen ausgewählt, für die Programmierkenntnisse nicht erforderlich waren.

7.2 Interesse der Schüler

Die am Wahlunterricht Kryptologie teilgenommenen Schüler gaben an, sich aus Neugier bzw. Interesse an Verschlüsselungen zu diesem Unterricht gemeldet zu haben. Weitere positive Einflussfaktoren waren die Teilnahme von Freunden, die zu dessen Besuch rieten, sowie Interesse an der Geschichte. Ein Schüler gab an, dass er mit einer Bemerkung über die Teilnahme am Wahlunterricht Kryptologie im Zeugnis, die Chancen auf einen Ausbildungsplatz als Informatiker erhöhen wollte. Doch nachdem er sich für den Besuch einer weiterführenden Schule entschieden hatte, nahm er am Wahlunterricht Kryptologie weiterhin teil, weil sein Interesse geweckt worden war.

Interesse an den einzelnen Themenbereichen
Im Hinblick auf die einzelnen Themenbereiche konnten die Schüler in einem Beurteilungsbogen angeben, ob sie die Themen

- sehr interessant (3 Punkte)
- interessant (2 Punkte)
- gering interessant (1 Punkt)
- völlig uninteressant (0 Punkte)

fanden. Anhand der Punktevergabe ist ein Durchschnittswert für jedes Thema zu errechnen, der in Abbildung 7.2 dargestellt wird. Die Beurteilung bezog sich dabei auf die folgenden Themenbereiche:

- Steganographie
- Caesar–Verschiebechiffre
- Einzelzeichen werden durch Einzelzeichen ersetzt
- Einzelzeichen werden durch mehrere Zeichen ersetzt
- Playfair–Verfahren/Codes
- Transpositionen
- Vigenère–Verschlüsselung
- Rotormaschinen: Enigma
- Vernam–Verschlüsselung
- RSA–Verfahren
- PGP–Verschlüsselung
- Integrität von Nachrichten
- Authentizität von Nachrichten

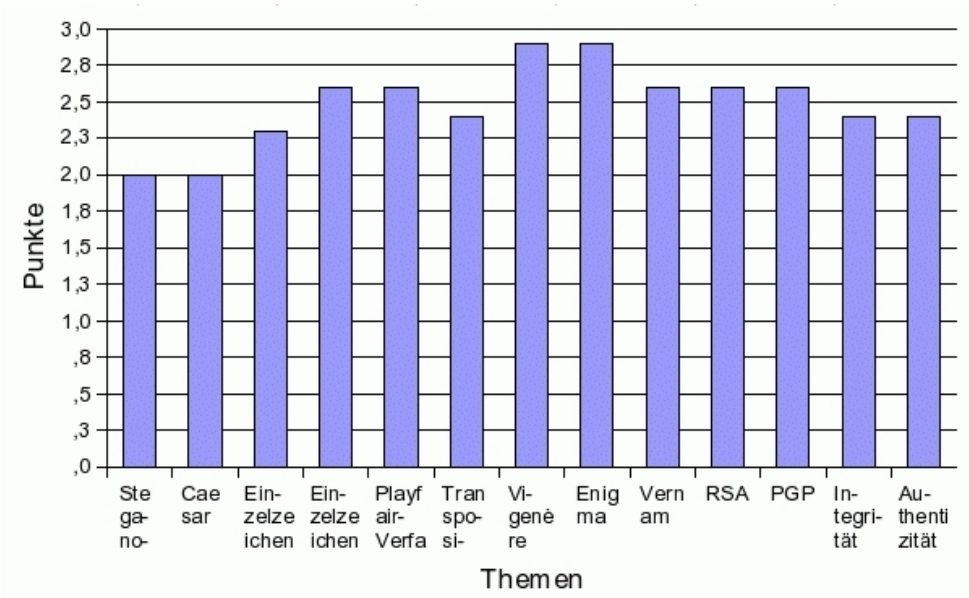


Abbildung 7.2: Interesse an den einzelnen Themenbereichen

Die Abbildung macht deutlich, dass die Verschlüsselung nach Vigenère sowie die Chiffriermaschine Enigma für Schüler besonders interessant sind. Gründe hierfür könnten sein, dass die Verschlüsselung nach Vigenère die erste Chiffre ist, die lange Zeit nicht entschlüsselt werden konnte und zu deren Dechiffrierung ein erhöhter Aufwand betrieben werden muss. Im Hinblick auf die Chiffriermaschine Enigma bringen Schüler bereits eigene Vorstellungen mit und sind

bestrebt, mehr über ihre Funktionsweise, Möglichkeiten des Angriffs und der damit zusammenhängenden geschichtlichen Ereignisse zu erfahren.

Neben der Steganographie weist auch die Caesar–Verschiebechiffre im Vergleich zu anderen kryptologischen Themen einen geringeren Grad an Interesse bei den Schülern auf. Die Ursache hierfür liegt bei der Caesar–Chiffre vermutlich in ihrer Einfachheit, die keine Sicherheit gewährleisten kann. Bei der Steganographie könnte das geringere Interesse bei Schülern daran liegen, dass sich diese Wissenschaft eben nicht mit Verschlüsselungen befasst, obwohl sich die Schüler auf das Erlernen von Geheimschriften eingestellt haben. Allerdings eignen sich beide Themengebiete aus didaktischen Gründen für den Einstieg in die Kryptographie. Anhand der Steganographie wird die Kryptographie als "offene" Verschlüsselung herausgestellt, bei der das Versenden einer Nachricht nicht verheimlicht wird. Die Verschiebechiffre nach Caesar bietet aufgrund der leichten Durchführbarkeit einen Einstieg in monographische Substitutionen an.

Insgesamt erreichen alle Themenbereiche Durchschnittswerte zwischen "interessant" und "sehr interessant", so dass die getroffene Auswahl an Themenbereichen der Kryptologie durchaus mit dem Interesse der Schüler übereinstimmt.

Themen mit dem größten Anklang
Neben der Beurteilung aller Themenbereiche wurden die Schüler auch danach befragt, welches Verschlüsselungsverfahren bzw. Thema ihnen am besten gefallen hat. Einhergehend mit den Angaben über das Interesse an den einzelnen Themenbereichen gab die Hälfte der Schüler die Enigma an, gefolgt von der Vigenère–Chiffre, die von 40% der Schüler genannt wurde.

Da der in dieser Arbeit vorgestellte Lehrplan[2)] für einen Unterricht in Kryptologie das Themengebiet "Die Enigma: Aufbau und Funktionsweise der Enigma; geschichtlicher Hintergrund" als Wahlpflichtbereich vorsieht, ist aufgrund des großen Interesses und des Anklangs bei Schülern dieses Thema in weiteren Unterrichtseinheiten in Kryptologie dringend zu empfehlen.

Die im Vergleich zu anderen Themengebieten weniger interessante Ausführung über die Steganographie wurde hier von einem Schüler zu den besten Themen des Wahlunterrichts gezählt. Dies ist wiederum ein Grund dafür, weshalb in einem Wahlunterricht Kryptologie ein Exkurs über Steganographie stattfinden sollte.

7.3 Beurteilung des Wahlunterrichts Kryptologie

Während des Schuljahres zeigten sich die am Wahlunterricht Kryptologie teilnehmenden Schüler sehr motiviert, was sich nicht nur in der regelmäßigen Anwesenheit, sondern auch in der Erledigung von zusätzlichen Aufgaben wie z. B. der Dechiffrierung von Kryptogrammen niederschlug.

Gegen Ende des Schuljahres konnten die Schüler den Unterricht in Kryptologie anhand eines Fragebogens anonym beurteilen. Dabei stellte sich heraus, dass die Erwartungen an den Wahl-

[2)] siehe Seite 45ff

unterricht Kryptologie bei allen Teilnehmern erfüllt wurden. Als Gründe führten die Schüler an, dass

- sie viel über Geheimschriften gelernt hätten,
- der Stoff mit Beispielen und Texten gut aufbereitet worden sei,
- der Stoff interessant gewesen sei und Spaß bereitet hätte.

Entsprechend gaben 70% der Schüler an, jüngeren Mitschülern zu empfehlen, den Wahlunterricht Kryptologie einmal zu besuchen. Die restlichen 30% würden ihre Empfehlung davon abhängig machen, ob Mitschüler hierin interessiert sind oder nicht.

Ob der Besuch des Unterrichts in Kryptologie praktischen Nutzen vermittelt hat, sollte die Frage klären, ob die Schüler auch später einmal Verschlüsselungsverfahren wie z. B. PGP in der Praxis anwenden werden. Hier waren sich die Befragten noch sehr unsicher. Die meisten Schüler, die sich mit Kryptologie weiter beschäftigen werden, sehen darin ein Hobby oder machen die Anwendung kryptographischer Methoden vom angestrebten Beruf abhängig. Die 30% der Teilnehmer, die Verschlüsselungsverfahren nicht anwenden werden, gaben an, dass sie zwar den Unterricht in Kryptologie interessant fanden, aber Verschlüsselungen wie PGP nicht brauchen werden.

Zusammenfassend ergibt sich damit von Seiten der Schüler eine positive Beurteilung des Unterrichts in Kryptologie. Auch wenn sich einige der Teilnehmer nicht weiter mit kryptologischen Verfahren beschäftigen werden, wurden die Erwartungen aller Schüler an den Wahlunterricht Kryptologie erfüllt und der Großteil von ihnen würde die Teilnahme weiter empfehlen.

7.4 Behaltensleistung

Gegen Ende des Schuljahres 2006/2007 wurde anhand eines Tests die Behaltensleistung bei kryptologischen Lerninhalten der am Wahlunterricht Kryptologie teilgenommenen Schüler überprüft. Im Folgenden werden diesbezüglich sowohl der Kenntnisstand der Teilnehmer dargestellt, als auch Problembereiche aufgezeigt.

7.4.1 Wissensstand bei kryptologischem Allgemeinwissen

Am Ende das Schuljahres ist bei den Schülern eine Fachsprache im Bereich der Kryptologie aufgebaut und gefestigt. Fachbegriffe wie z. B. Kryptographie, Kryptanalyse, Steganographie usw. werden von den Schülern nicht nur aktiv verwendet; sie können auch ihre Bedeutung in eigenen Worten sehr gut erklären.

Daneben sind die Schüler in der Lage, Relationen, die eine Verschlüsselung darstellen von solchen Zuordnungen zu unterscheiden, die den Anforderungen einer Verschlüsselung nicht genügen. Auch die Begründung, dass eine Relation keine Verschlüsselung darstellt, falls sie nicht eindeutig umkehrbar ist, wurde von allen Teilnehmern richtig angegeben.

Schließlich weisen die Teilnehmer grundlegende Kenntnisse bei der Einteilung beispielhafter Chiffren in die Bereiche der symmetrischen und asymmetrischen Chiffrierverfahren sowie bei symmetrischen Verfahren in Transpositionen und Chiffren durch Substitution auf.

7.4.2 Wissensstand bei symmetrischen Chiffrierverfahren

Monoalphabetische Chiffrierverfahren
Im Bereich der monoalphabetischen Chiffrierverfahren sind die Schüler in der Lage, die Funktionsweise besprochener Chiffrierverfahren wiederzugeben. So wurde von allen Schülern sowohl die Caesar–Verschiebechiffre als auch monographische Chiffren allgemein sehr gut erklärt. Bei der Frage, worauf bei der Vorschrift der Verschlüsselung zu achten ist, wenn Einzelzeichen durch mehrere Geheimtextzeichen ersetzt werden, wurde von allen Teilnehmern richtig geantwortet, dass keinem Geheimtextzeichen zwei Klartextbuchstaben zugeordnet werden dürfen.

Neben den Kenntnissen über die Verschlüsselung konnten alle Teilnehmer die Vorgehensweise in der Kryptanalyse bei monoalphabetischen Substitutionen sehr gut erklären. Dass durch die Häufigkeit von einzelnen Geheimtextzeichen sowie von Bigrammen Rückschlüsse auf die Klartextzeichen gezogen werden können, ist allen Schülern bekannt. Allerdings zeigten sich Wissenslücken bei der Entschlüsselung eines Kryptogramms, das durch eine Spalten–Transposition erzeugt wurde. Hier ist im Unterricht stärker zu betonen, dass bei einer Spalten– bzw. Zeilen–Transposition das Kryptogramm durch eine Aneinanderreihung des ersten, zweiten usw. Buchstabens aus jedem Buchstaben–Block gebrochen werden kann.

Polyalphabetische Chiffrierverfahren
Im Bereich der polyalphabetischen Chiffrierverfahren waren alle Teilnehmer in der Lage, einen vorgegebenen Klartext richtig nach Vigenère zu verschlüsseln. Dabei war das Vigenère–Schlüsselwort festgelegt und ein Vigenère–Quadrat vorgegeben.

Im Unterricht wurde besprochen, dass die Sicherheit der Vigenère–Verschlüsselung durch sehr lange Schlüsselwörter erhöht werden kann. Im Test gaben diesbezüglich zwei Schüler an, dass die Sicherheit durch mehrmaliges Verschlüsseln erhöht werden könnte, was bei Verwendung unterschiedlicher Schlüsselwörter grundsätzlich nicht falsch ist.

Daneben zeigte sich bei einem häuslichen Arbeitsauftrag, dass die Schüler in der Lage sind, ein nach Vigenère verschlüsseltes Kryptogramm mit einem fünfstelligen Schlüsselwort ohne Kenntnis des Schlüssels zu entschlüsseln.

Bei Fragen zur Chiffriermaschine Enigma sind alle Schüler in der Lage, drei Einstellmöglichkeiten zu nennen und die Aufgabe der Umkehrwalze anzugeben. Wissenslücken zeigten sich bei der Frage, welchen Nachteil die Umkehrwalze mit sich bringt.

7.4.3 Wissensstand bei asymmetrischen Chiffrierverfahren

Im Bereich der asymmetrischen Chiffrierverfahren wurde im Test überwiegend der Kenntnisstand beim RSA–Verfahren geprüft. Da die Hälfte der Teilnehmer die Verschlüsselungssoftware

PGP auch auf dem eigenen Computer zu Hause installiert hat, kann davon ausgegangen werden, dass Kenntnisse im Umgang mit dieser Software vorhanden sind.

Bei der Erzeugung eines Schlüsselpaares zum RSA–Verfahren zeigte sich, dass Schüler der Realschule an ihre mathematischen Leistungsgrenzen gelangen. So bedurfte es nicht nur im Unterricht einer starken Unterstützung durch die Lehrkraft; auch im Test hatten viele Schüler hierin Schwierigkeiten. Dies bedeutet auch, dass noch komplexere Verschlüsselungsverfahren für den Schulunterricht ungeeignet sind.

Bei einem vorgegebenen Schlüsselpaar sind die Schüler in der Lage, (mithilfe des Taschenrechners) eine Zahl mit RSA zu verschlüsseln bzw. zu entschlüsseln. Auch das experimentelle Erfassen des Zeitaufwands beim Faktorisieren von Zahlen scheint Eindruck hinterlassen zu haben. Die meisten Schüler konnten erklären, worauf die Sicherheit des RSA–Verfahrens beruht.

7.5 Zusammenfassung

In diesem Kapitel werden Praxiserfahrungen dargelegt, die während der Durchführung eines Wahlunterrichts Kryptologie im Schuljahr 2006/2007 an der Städtischen Elly–Heuss–Realschule in München gesammelt wurden. Es zeigt sich, dass sich vor allem Schüler des mathematisch–naturwissenschaftlichen Ausbildungszweiges für Kryptologie interessieren.

Die in dieser Arbeit ausgewählten Themenbereiche der Kryptologie finden bei Schülern großen Zuspruch, wobei sich die Schüler insbesondere für die Verschlüsselung nach Vigenère und die Chiffriermaschine Enigma interessieren. Geringeres Interesse wird im Durchschnitt der Verschlüsselung nach Caesar und der Steganographie entgegen gebracht.

Allgemein wird der Wahlunterricht Kryptologie von Schülern positiv beurteilt, was sich nicht nur in ihrer Motivation niederschlägt, sondern auch darin zeigt, dass die meisten Teilnehmer anderen Schülern den Besuch des Wahlunterrichts empfehlen würden.

Bei einem abschließenden Test zeigten die Schüler sehr gute Kenntnisse im Bereich über kryptologisches Allgemeinwissen sowie bei symmetrischen Chiffrierverfahren. Selbst aufwendigere polyalphabetische Chiffren wie die Vigenère–Verschlüsselung können die Schüler nicht nur erzeugen, sondern auch brechen. Bei Berechnungen im Bereich der asymmetrischen Verfahren wie z. B. der Schlüsselerzeugung beim RSA–Verfahren ist bei Realschülern Unterstützung durch die Lehrkraft erforderlich.

8 Zusammenfassung

Im heutigen Informationszeitalter erfährt die Kryptologie zunehmend praktische Bedeutung. So werden über kryptographische Verfahren z. B. bei Mobilfunknetzen und beim Pay–TV die berechtigte Benutzung sichergestellt, digitale Datenträger mit Kopierschutz versehen sowie die Datenübertragung beim Online–Banking oder per E–Mail geschützt. Gleichzeitig bieten moderne kryptologische Verfahren Möglichkeiten zur Überprüfung von Authentizität und Integrität beim Nachrichtenaustausch und ermöglichen elektronische Signaturen.

Die schulische Ausbildung hinsichtlich der Kryptologie ist allerdings sehr begrenzt. Kryptologie wird in den meisten Lehrplänen nicht erwähnt, obwohl neben dem Alltagsbezug zahlreiche fächerübergreifende unterrichtliche Einsatzmöglichkeiten bestehen.

Moderne Verfahren der Kryptographie stützen sich auf die Zahlentheorie, deren Grundlagen im Mathematikunterricht der Sekundarstufe I behandelt werden. Kryptographische Algorithmen bieten die Entwicklung von Verschlüsselungssoftware im Informatikunterricht an. Aufgrund der jahrtausende alten Vergangenheit erscheinen geschichtliche Ereignisse unter einer anderen Perspektive, die im Unterricht Geschichte aufgezeigt werden kann. Die rechtliche Lage im Hinblick auf den Einsatz von Verschlüsselungssoftware und Datenschutz bietet eine unterrichtliche Verbindung zum Fach Wirtschaft und Recht an. Schließlich existieren zahlreiche Beispiele von Geheimschriften in der Literatur, so dass ein Bezug zum Unterrichtsfach Deutsch möglich ist.

Trotz der gegenwärtigen Bedeutung kryptographischer Methoden und positiven fächerübergreifenden Einsatzmöglichkeiten können kryptologische Inhalte nur dann Eingang in den Schulunterricht finden, wenn sie einen Beitrag zum Bildungs- und Erziehungsauftrag der Schulen leisten. Dies erfordert die Unterstützung der Allgemeinbildung, der Berufsvorbereitung und der Studienvorbereitung. In dieser Arbeit wird nachgewiesen, dass ein Wahlunterricht Kryptologie den Anforderungen der Allgemeinbildung genügt und einen Beitrag zur Berufs- bzw. Studienvorbereitung leistet.

Ausgehend von der Berechtigung eines Unterrichts in Kryptologie wird der didaktische Ort für einen entsprechenden Wahlunterricht erörtert. Die notwendigen mathematischen Vorkenntnisse verweisen diesen Unterricht auf die Jahrgangsstufen 9 bis 12. Ausgehend von einem zweistündigen Wahlunterricht werden anschließend Lerninhalte von Kryptologie an Hauptschulen sowie an Realschulen und Gymnasien bestimmt und entsprechend einem Lehrplan in eine zeitliche Abfolge gebracht. Zudem werden Wahlpflichtbereiche vorgesehen, die eine innere Differenzierung zwischen Schülern mit und ohne Programmiererfahrung ermöglichen.

In dieser Arbeit werden Beispiele für die unterrichtliche Umsetzung der festgelegten kryptologischen Lerninhalte dargelegt. In Anlehnung an die Berliner–Didaktik werden ausgehend von

den Lernzielen, Inhalte aufgezeigt, mit denen diese Intentionen erreicht werden können und mit methodischen Hinweisen versehen.

Als Einführung in einen Unterricht in Kryptologie wird die Darlegung der Ziele der Kryptographie sowie deren Umsetzung mit praktischen Beispielen vorgeschlagen. Daneben sind zum Aufbau einer Fachsprache die Einführung von Fachbegriffen vorgesehen, wobei die Verschlüsselung als Relation dargestellt wird, die einen Klartext in einen Geheimtext überführt. Um Verwechslungen zum "verdeckten" Nachrichtenaustausch zu vermeiden, wird über eine Einführung in die Steganographie die Kryptographie hiervon abgegrenzt.

Entsprechend der geschichtlichen Entwicklung werden zunächst symmetrische Chiffrierverfahren behandelt. Ausgehend von der Verschiebechiffre nach Caesar werden monoalphabetische Chiffrierverfahren vorgestellt. Neben dem Ersetzen von Klartextbuchstaben im Rahmen der Substitutionschiffren lernen Schüler auch Transpositionen kennen, die durch eine Veränderung der Buchstabenposition eine Nachricht verschlüsseln. Im Bereich der polyalphabetischen Chiffrierverfahren wird besonderer Wert auf die Vigenère–Verschlüsselung sowie auf die Rotormaschine Enigma gelegt.

Da nach Einführung einer kryptographischen Methode auch Aspekte zum Brechen dieser Chiffre aufgezeigt werden, erkennen die Schüler die Schwächen einer Verschlüsselungsmethode und stellen Überlegungen zu deren Verbesserung an. Auf diese Weise gelangt man von der Chiffre nach Vigenère zur Vernam–Verschlüsselung, die perfekte Sicherheit gewährleistet.

Die Nachteile symmetrischer Chiffrierverfahren führen zur Entwicklung der asymmetrischen Kryptologie, für die ebenfalls eine Unterrichtssequenz vorgestellt wird. Da asymmetrische Verfahren auf der Modulo–Rechnung beruhen, wird diese zunächst eingeführt, bevor die Notwendigkeit von Einweg–Funktionen aufgezeigt wird. Die Einweg–Eigenschaft der Produktbildung großer Primzahlen, auf der das RSA–Verfahren beruht, wird experimentell mit einem Computeralgebrasystem nachgewiesen. Die Einweg–Eigenschaft der diskreten Exponentialfunktion wird durch die Untersuchung von Berechnungsmethoden plausibel gemacht. Neben dem Diffie–Hellman–Schlüsselaustausch wird in dieser Arbeit die unterrichtliche Behandlung des RSA–Verfahrens vorgeschlagen. Hierfür sind zur Schlüsselerzeugung Elemente der Zahlentheorie wie z. B. die Eulersche ϕ–Funktion sowie der euklidische Algorithmus einzuführen. Aus Gründen der Motivation wird anschließend der unterrichtliche Einsatz der Verschlüsselungssoftware PGP vorgeschlagen. Die Entstehungsgeschichte macht in besonderer Weise auf Vor- und Nachteile der privaten Datenverschlüsselung aufmerksam. Hier ist vorgesehen, auf die Rechtslage hinsichtlich dem Gebrauch kryptographischer Methoden einzugehen.

Da sich die bisherigen Unterrichtsbeispiele auf die Vertraulichkeit beim Nachrichtenaustausch beschränken, wird nun auch eine Unterrichtssequenz zu "Authentizität und Integrität" vorgestellt. Hinsichtlich der Gewährleistung von Nachrichtenintegrität wird die Konstruktion von Hashfunktionen dargelegt sowie das in der Praxis angewandte MD5–Verfahren analysiert. Danach ist die Sicherstellung der Nachrichtenauthentizität sowohl mit dem Message Authentication Code als auch mit digitalen Signaturen vorgesehen. In Anlehnung an die behandelten asymmetrischen Kryptosysteme wird in diesem Kapitel die Funktionsweise elektronischer Signaturen ebenfalls bei RSA- sowie bei PGP–Verfahren erläutert. Zur Sicherstellung der Benutzerauthentizität wird sowohl das Passwortverfahren als auch das Challenge–and–Response–

Verfahren vorgestellt. Die Unterrichtssequenz endet mit einer Einführung in Zero–Knowledge–Protokolle.

Da die vorgestellten Unterrichtsbeispiele in einem Wahlunterricht Kryptologie praktisch erprobt wurden, werden schließlich Erkenntnisse dargelegt, die während des Schuljahres 2006/2007 an der Städtischen Elly–Heuss–Realschule in München gesammelt wurden. Es zeigt sich, dass die teilnehmenden Schüler mehrheitlich den naturwissenschaftlichen Ausbildungszweig besuchen und an der Vigenère–Verschlüsselung sowie der Enigma besonders interessiert sind. Insgesamt wird der Wahlunterricht Kryptologie von Seiten der Schüler positiv beurteilt. In einem abschließenden Test zeigten die Schüler sehr gute Kenntnisse bei symmetrischen Chiffrierverfahren. Im Bereich der asymmetrischen Kryptographie ist bei schwierigeren Berechnungen Unterstützung durch die Lehrkraft erforderlich.

9 Anhang

Anhang A

Programmierung der Caesar–Verschiebechiffre mit Visual Basic

Voraussetzung für das Entwerfen des vorgestellten Programms zur Caesar–Chiffre sind Kenntnisse zu Ein- und Ausgabeanweisungen, Zuweisungen, Wiederholungsanweisungen, Bedingungen und String–Funktionen in der Programmiersprache Visual Basic.

Daneben ist die Kenntnis über die Darstellung von Buchstaben in einem Computer in Form des ASCII–Codes[1)] erforderlich. Der ASCII–Code kann auch in der Vorstunde zur Programmierung der Caesar–Chiffre besprochen werden. Wichtig ist dabei die Erkenntnis, dass die Großbuchstaben von A bis Z in ASCII durch die Zahlen 65 bis 90 und die Kleinbuchstaben von a bis z durch die Zahlen 97 bis 122 codiert werden.

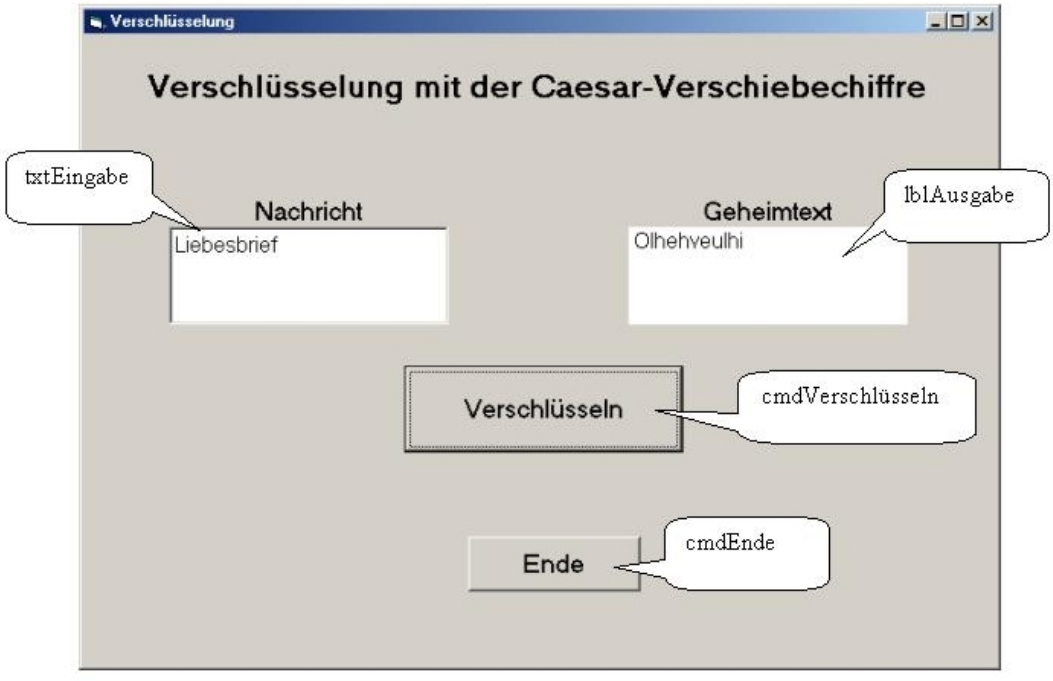


Abbildung 9.1: Bildschirmlayout und Objekte

[1)] American Standard Code for Information Interchange

Die Entwicklung eines Programms beginnt im Unterricht mit der Erstellung des Struktogramms, d. h. einem Entwurf der Software. Hierbei werden neben dem Algorithmus auch die erforderlichen Variablen sowie die erforderlichen Funktionen herausgearbeitet.

Liste der Variablen		
Name	**Datentyp**	**Bemerkung**
laenge	integer	Länge der Eingabe
l	integer	Laufvariable der For–Schleife
i	integer	ASCII–Code des Buchstabens
buchstabe	string	zu verschlüsselnder Buchstabe der Eingabe
gtext	string	Geheimtext

Zeichenkettenfunktionen		
Funktion	**Syntax**	**Bedeutung**
Asc	Asc(a)	Ermittelt den ASCII–Code eines Stringzeichens a. Besteht der String aus mehr als einem Zeichen, wird nur das erste Zeichen verwendet.
Chr	Chr(b)	Wandelt den Zeichencode b (0 bis 255) in einen 1-Zeichen-String um.
Mid	Mid(String, n, Anzahl)	Trennt ab der Position n Anzahl Zeichen aus dem String heraus und gibt sie als String zurück.

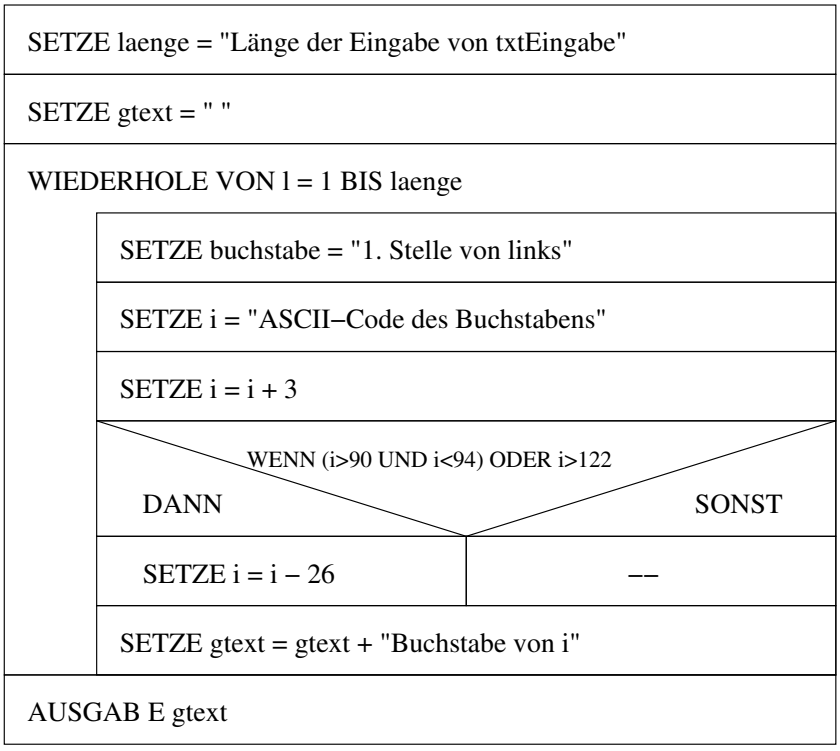


Abbildung 9.2: Struktogramm zum Caesar–Verschlüsselungsprogramm

```
Option Explicit
        Private laenge As Integer, l As Integer, i As Integer
        Private buchstabe As String, gtext As String
```

```
Private Sub cmdVerschlüsseln_Click()
        laenge = Len(txtEingabe)
        gtext = " "
        For l = 1 To laenge
                buchstabe = Mid(txtEingabe,l,1)
                i = Asc(buchstabe)
                i = i+3
                If (i>90 And i<94) Or i>122 Then
                        i = i – 26
                End If
                gtext = gtext + Chr(i)
        Next l
        lblAusgabe.Caption = gtext
End Sub
```

```
Private Sub cmdEnde_Click()
        End
End Sub
```

Abbildung 9.3: Prozedur–Code zur Caesar–Chiffre

Anhang B

Auszug aus “Der Goldkäfer” von Edgar Allan Poe

In der Erzählung “Der Goldkäfer” ist vom Piraten Kapitän Kidd in einer Geheimschrift die Lage eines Schatzes beschrieben. Dass es sich um einen Bericht von Kapitän Kidd (Kid = Geißlein) handelt, ist an einer verschlüsselten Unterschrift in Form einer Ziege zu erkennen. Das Kryptogramm ist mithilfe einer Geheimtinte unsichtbar und wird durch Erhitzen lesbar. Im folgenden Textausschnitt berichtet der Held Legrand, wie er den Schatz ausfindig gemacht hat:

“Hiermit überließ mir Legrand das Pergament, das er wiederum erhitzt hatte, zur Begutachtung. Zwischen dem Totenkopf und der Ziege zeigten sich in roter Farbe ungelenke Zeichen, die dieses Bild ergaben:

$53‡‡†305))6*,4826)4‡.)4‡);806*;48†8\pi60))85;1‡(;:‡*8†83\ (88)5*†;46(;88*96*?;8)*‡(;485);5*†2:*‡\ (;4956\ *\ 2(5\ *\ -4)\ 8\pi8*;\ 4069285)\ ;)6\ †\ 8)\ 4\ ‡\ ‡;\ 1(‡9;\ 48081;\ 8\ :\ 8\ ‡\ 1;\ 48\ †\ 85;\ 4)\ 485\ †\ 528806\ *\ 81(‡9;48;(88;4(‡?34;48)4‡;161;:188;‡?;$

“Aber”, sagte ich, indem ich ihm den Zettel zurückgab, “ich tappe nach wie vor im dunkeln. Und wenn mir alle Juwelen von Golconda für die Lösung dieses Rätsels geboten würden, wäre ich trotzdem außerstande, sie zu erringen.”
“Und doch”, sagte Legrand, “ist die Lösung gar nicht so schwer, wie Sie nach der ersten flüchtigen Betrachtung der Zeichen vermuten. Diese Zeichen bilden, wie sich leicht erraten lässt, eine Geheimschrift, das heißt, sie haben etwas zu bedeuten. Nach allem, was mir von Kidd bekannt ist, konnte ich jedoch nicht annehmen, dass er fähig gewesen sei, eine besonders schwierige Geheimschrift zu ersinnen. Ich sah gleich, dass diese hier zu der einfachen Gattung gehörte, die freilich dem groben Verstand eines Seemanns ohne den Schlüssel völlig unlösbar erscheinen musste.”
“Und Sie haben sie wirklich gelöst?”
“Allerdings. [...] Im vorliegenden Fall – wie übrigens immer bei allen Geheimschriften – lautet die erste Frage, in welcher Sprache die Geheimschrift abgefasst ist; denn die Lösungen richten sich, besonders wenn es sich um einfachere Geheimschriften handelt, nach dem Geist der jeweiligen Sprache und sind dementsprechend veränderlich. Im allgemeinen bleibt keine Wahl als das auf Wahrscheinlichkeit gestützte Probieren mit jeder Sprache, die demjenigen bekannt ist, der die Lösung sucht, bis er auf die richtige stößt. Im Falle unseres Schlüsseltextes wurden jedoch alle Schwierigkeiten von vornherein durch die Unterschrift beseitigt. Das Wortspiel “Kidd” ist nur in der englischen Sprache möglich. [...] Sie bemerken, dass die Wörter nicht voneinander getrennt sind. Wäre dies der Fall gewesen, so hätte ich verhältnismäßig wenig Mühe gehabt. Ich hätte dann mit dem Vergleichen und Zerlegen der kürzeren Wörter begonnen, und wäre – was wahrscheinlich ist – ein Wort mit einem einzigen Buchstaben (zum Beispiel a oder I) vorgekommen, so hätte ich die Lösung als gesichert betrachtet. Da aber keine Worttrennungen zu erkennen waren, musste ich zunächst die am häufigsten und die am seltensten erscheinenden Zeichen ermitteln. Ich zählte alle und stellte darauf diese Liste zusammen:

Das Zeichen	8 erscheint 33mal
	; erscheint 26mal
	4 erscheint 19mal [...]

Nun kommt im Englischen der Buchstabe e am häufigsten vor. Die weitere Reihenfolge ist: a o i d h n r s t u y c f g l m w b k q p x z. Das e überwiegt so auffallend, dass es keinen einigermaßen langen Satz gibt, in welchen es nicht den häufigsten Buchstaben bildet. [...] Da das vorherrschende Zeichen 8 ist, wollen wir damit beginnen, es als das e des Alphabets zu betrachten. Zur Bestätigung unserer Annahme wollen wir feststellen, ob das Zeichen 8 öfters paarweise erscheint; denn das e wird im Englischen häufig verdoppelt, wie zum Beispiel in “meet”, “fleet”, “speed”, “seen”, “been”, “agree” und so weiter. In unserem Falle stellen wir nicht weniger als fünf Verdoppelungen fest, obgleich es sich nur um einen kurzen Text handelt.
Nehmen wir also das Zeichen 8 als e an. Nun ist das gebräuchlichste aller Wörter der Artikel the; sehen wir also

nach, ob es Wiederholungen dreier Zeichen gibt, deren letztes 8 ist. Wenn wir Wiederholungen solcher Zeichen in gleicher Anordnung entdecken, stellen diese höchstwahrscheinlich das Wort “the” dar. Beim Nachprüfen finden wir nicht weniger als sieben solcher Anordnungen, bestehend aus den Zeichen ;48. Wir können also annehmen, dass ;t, 4h und 8e bedeutet – womit die Richtigkeit dieses letzten Zeichens bestätigt wäre. Damit ist ein großer Schritt vorwärts getan.
Nachdem wir aber ein einzelnes Wort ermittelt haben, sind wir imstande, einen ungeheuer wichtigen Punkt, das heißt, mehrere Anfänge und Endungen anderer Wörter festzulegen. Beziehen wir uns zum Beispiel auf den vorletzten Fall, in welchem die Verbindung ;48 – ziemlich am Schluss des Textes – erscheint. Wir wissen, dass das ;, das unmittelbar folgt, den Anfang eines neuen Wortes bildet; von den sechs Zeichen, die diesem “the” folgen, sind uns nicht weniger als sechs Zeichen bekannt. Schreiben wir also diese Zeichen auf, indem wir die uns bereits bekannten Buchstaben einsetzen und für den noch unbekannten einen freien Raum lassen:

t eeth.

Hier können wir sofort das th abtrennen, da es keinen Teil des Wortes, das mit dem ersten t anfängt, bildet. Denn wenn wir das ganze Alphabet durchprobieren, um einen in den Leerraum passenden Buchstaben zu ermitteln, erkennen wir, dass es kein Wort gibt, von dem dieses th ein Teil sein kann. Wir sind also beschränkt auf

t ee,

und wir gelangen, wenn wir – falls nötig – wie vorher das Alphabet durchgehen, zum Worte “tree” als einzig möglichem. Dadurch gewinnen wir einen weiteren Buchstaben, das r, dargestellt durch (, zusammen also die beiden Wörter: the tree.
Wenn wir ein kurzes Stück weitergehen, stoßen wir wiederum auf die Verbindung ;48 und verwenden sie als Schluss des unmittelbar Vorhergehenden. Wir bekommen also die Anordnung:

the tree ;4(‡?34 the,

oder, wenn wir die uns schon bekannten Buchstaben einsetzen;

the tree thr‡?3h the.

Wenn wir jetzt an Stelle der unbekannten Buchstaben freien Raum lassen oder diesen durch Punkte bezeichnen, lesen wir:

the tree thr...h the,

worauf wir sofort das Wort “through” erkennen. Diese Entdeckung verschafft uns jedoch drei neue Buchstaben, o, u, g, dargestellt durch die Zeichen ‡, ? und 3.
Sehen wir jetzt den Text nach Verbindungen bekannter Zeichen durch, so begegnet uns ziemlich am Anfang die Anordnung:

83(88, oder egree,

was offenbar der Schluss des Wortes “degree” ist und uns einen neuen Buchstaben, d, dargestellt durch †, gibt.[...]
Ich will Ihnen nur noch die volle Übersetzung des auf dem Pergament befindlichen ungelösten Textes geben. Sie lautet folgendermaßen:
«A good glass in the bishop’s hostel in the devil’s seat forty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death’s-head a bee-line from the tree through the shot fifty feet out.»”[2)]

[2)] [28], S. 201ff

Anhang C

Geheimschrift der Maria Stuart

Abbildung 9.4: Chiffre von Maria Stuart

Wie obige Abbildung zeigt, war die Geheimschrift der Maria Stuart eine monoalphabetische Chiffre, die jedem Klartextbuchstaben genau ein Zeichen zuordnete. Dabei wurden die Buchstaben j, v und w in einer Nachricht weggelassen. Daneben konnten Buchstaben–Verdopplungen vermieden werden, da das Symbol “Dowbleth” Doppelbuchstaben anzeigte.

Als Blender dienten die Zeichen, die mit “Nulles” gekennzeichnet sind. Die Wörter and, for, with usw. dienten als Spreizer – auch als Codewörter bezeichnet – und wurden jeweils durch ein Geheimtextzeichen ersetzt.

Anhang D

Auszug aus “Reise zum Mittelpunkt der Erde” von Julius Verne

Der Roman “Reise zum Mittelpunkt der Erde” handelt von einer abenteuerlichen Expedition des Professors Lidenbrock und seines Neffen Axel ins Innere der Erde. Der Weg hierzu wird durch ein verschlüsseltes, altes Dokument des isländischen Gelehrten Arne Saknussemm beschrieben. Im folgenden Textausschnitt stellt Professor Lidenbrock Überlegungen zur Entzifferung des Dokuments an.

“Mir scheint”, sagte er, “der erste Gedanke, auf den man kommt, um die Buchstaben eines Satzes durcheinanderzubringen, ist, die Worte vertikal statt horizontal zu schreiben.”
“So etwas!” dachte ich.
“Man muss sehen, was dabei herauskommt. Axel, schreib irgendeinen Satz auf dieses Stück Papier, aber statt die Buchstaben aneinanderzufügen, schreib sie vertikal untereinander, und zwar in Gruppen von fünf bis sechs.”
Ich verstand, was er meinte, und schrieb sofort von oben nach unten:

I b e e i
c e k G n
h m l r n
l e e e i
i i i t g
e n n e

Abbildung 9.5: Leicht veränderter Auszug aus “Reise zum Mittelpunkt der Erde”

“Gut”, sagte der Professor, ohne es gelesen zu haben. “Jetzt schreibe diese Buchstaben in eine waagrechte Zeile.”
Ich gehorchte, und es wurde folgender Satz daraus:

Ibeei cekGn hmlrn leeei iiitg enne

“Ausgezeichnet”, sagte mein Onkel und riss mir das Stück Papier aus der Hand, “das sieht schon aus wie das alte Dokument; die Vokale sind wie die Konsonanten im gleichen Durcheinander gruppiert; es gibt sogar einen großen Buchstaben, genau wie auf dem Saknussemm–Pergament.”
Ohne es zu wollen, fand ich das, was er sagte, scharfsinnig.
“Nun”, fuhr mein Onkel fort, sich direkt an mich wendend, “um den Satz zu lesen, den du soeben geschrieben hast und den ich nicht kenne, brauche ich nur den ersten Buchstaben aller Wörter aneinanderzureihen, dann den zweiten, dann den dritten usw.”
Und zu meinem und vor allem seinem großen Erstaunen las mein Onkel:
“Ich liebe meine kleine Grete innig.”
“Na, na”, sagte der Professor.
Ohne es zu ahnen, hatte ich verliebter Tölpel diesen verräterischen Satz geschrieben.[3)]

[3)] [33], S. 19

Anhang E

Auszug aus “Mathias Sandorf” von Julius Verne

Der Roman “Mathias Sandorf” handelt von einer Gruppe von Verschwörern, die im Jahre 1867 Ungarn von der österreichischen Herrschaft befreien wollen. Der folgende Auszug beginnt bei der Dechiffrierung einer verschlüsselten Brieftaubenpost.

Der Vorgang war einfach: Bei Anwendung der Gitter–Methode[4)] behält jeder Buchstabe seinen alphabetischen Wert; ein “b” oder ein “o” wird auch als “b” beziehungsweise “o” gelesen. Man legt ein Gitter mit einer bestimmten Anzahl offener und geschlossener Felder über das verschlüsselte Wort und notiert zunächst nur hintereinander die Buchstaben, die in den offenen Feldern erscheinen. Nun macht man mit dem Gitter eine Vierteldrehung, schreibt die Buchstaben auf, die diesmal in den Fenstern erscheinen, dreht das Gitter weiter, schreibt die neuen Buchstaben auf und fährt so fort, bis alle Buchstaben der Botschaft notiert sind. Fortlaufend gelesen ergeben sie dann den sinnvollen Text.
Solche Gitter wurden schon in alten Zeiten verwendet. Man hat sie nur neuerdings [...] vervollkommnet. Auf jeden Fall sind sie all jenen Systemen überlegen, in denen man jeweils nur einen bestimmten Buchstaben zur neuen Basis des Alphabets erhebt oder überhaupt nur vorher von den Partnern festgelegte Buchstaben gegeneinander austauscht. Gute Dechiffrierer können über solche Methoden nur lächeln. Durch bloßes Probieren und Raten, durch Wahrscheinlichkeitsrechnungen und andere Tricks kommen sie den meisten Geheimsprachen auf die Spur. Allein aus der Häufigkeit bestimmter Buchstaben ziehen sie Rückschlüsse auf die Sprache, in der die Botschaft abgefasst sein könnte. Zahlreiche “e” sprechen beispielsweise für einen französischen, englischen oder deutschen Text, gehäufte “o” für einen spanischen, viele “a” für einen russischen und das gleichzeitige Auftreten vieler “e” und “i” für einen italienischen.
Kein Wunder also, dass man dergleichen Systeme heute gern meidet und lieber mit den bereits erwähnten Gittern oder auch mit chiffrierten Wörterbüchern arbeitet, in denen einzelne gebräuchliche Wörter für ganze Satzeinheiten stehen, aber ihrerseits schon wieder durch Zahlen ersetzt sind. Die beiden letztgenannten Systeme haben aber auch eine bedenkliche Schwäche: Ihre Benutzer sind verpflichtet, um keinen Preis das Gitter oder das Wörterbuch zu verlieren oder in unrechte Hände gelangen zu lassen, denn wer im Besitz dieser Hilfsinstrumente ist, kann auch jede Botschaft in der dazugehörigen Schlüsselsprache entziffern.[5)]

Julius Verne erklärt in einem späteren Abschnitt die genaue Funktionsweise des Drehrasters:

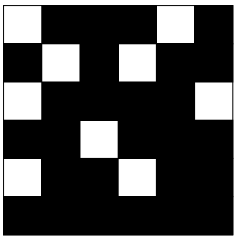


Abbildung 9.6: Raster aus Julius Verne “Mathias Sandorf”

In den neun offenen Feldern waren zunächst nur neun Buchstaben ablesbar; die übrigen siebenundzwanzig blieben verdeckt. Bei einer Vierteldrehung der Karte im Uhrzeigersinn mussten wiederum neun Buchstaben erscheinen. Wiederholte man diese Vierteldrehungen noch zweimal, wären zum Schluss alle sechunddreißig Buchstaben in

[4)] Raster–Transposition; statt “Raster” verwendet der Autor den Begriff “Gitter”.
[5)] [34], S. 31/32

nunmehr neuer Reihenfolge ablesbar geworden. Der Einfachheit halber sollte der Leser diese Methode mit Hilfe von Zahlen erproben. Man unterlege das oben abgebildete Gitter mit einem Blatt Papier und trage in die neun offenen Felder die Zahlen 1 bis 9 fortlaufend ein. Nach der ersten Vierteldrehung schreibe man die Zahlen 10 bis 18 in die leeren Quadrate, nach der zweiten Drehung die Zahlen 19 bis 27 und nach der letzten Drehung die Zahlen 28 bis 36. Hebt man das Gitter ab, findet man die Zahlen 1 bis 36 über die sechunddreißig Felder des Gitters verteilt, wobei stets nur eine Zahl auf ein Quadrat entfällt.[6)]

[6)] [34], S. 56

Anhang F

Bastelanleitung für ein einfaches Rotorgerät

Das von R. Matthews in [24] vorgestellte Rotorgerät besteht im wesentlichen aus zwei Papierstreifen, wie sie in Abbildung 9.7 wiedergegeben sind. Diese Papierstreifen weisen drei Einteilungen auf:
Auf dem linken Streifen sind in der Spalte “2” die 25 Buchstaben des Alphabets – ohne dem Buchstaben Q – aufgelistet, und in der Spalte “1” ist die Position des jeweiligen Buchstabens im Alphabet notiert. Der rechte Streifen besteht aus allen Zahlen von 0 bis 99, die derart zusammengestellt sind, dass die Zahlen in einer Zeile denselben Rest modulo 25 ergeben.

0	A	1, 26, 51, 76
1	B	←, 25, 50, 75
2	C	24, 49, 74, 99
3	D	23, 48, 73, 98
4	E	22, 47, 72, 97
5	F	21, 46, 71, 96
6	G	20, 45, 70, 95
7	H	19, 44, 69, 94
8	I	18, 43, 68, 93
9	J	17, 42, 67, 92
10	K	16, 41, 66, 91
11	L	15, 40, 65, 90
12	M	14, 39, 64, 89
13	N	13, 38, 63, 88
14	O	12, 37, 62, 87
15	P	11, 36, 61, 86
16	R	10, 35, 60, 85
17	S	9, 34, 59, 84
18	T	8, 33, 58, 83
19	U	7, 32, 57, 82
20	V	6, 31, 56, 81
21	W	5, 30, 55, 80
22	X	4, 29, 54, 79
23	Y	3, 28, 53, 78
24	Z	2, 27, 52, 77
“1”	“2”	“3”

Abbildung 9.7: Kopiervorlage: Papierstreifen des Rotorgerätes

Diese (an der horizontalen Linie getrennten) Papierstreifen werden um eine zylinderförmige Walze gewickelt und an beiden Enden zusammengeklebt. Als Walze schlägt Matthews die Dose eines Kleinbildfilms vor (vgl. Abbildung 9.8).

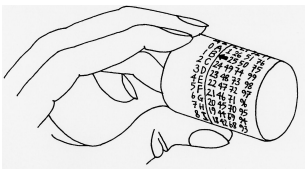


Abbildung 9.8: Die Papierstreifen werden um eine zylinderförmige Dose gewickelt.

Die Verschlüsselung erfolgt nun mithilfe von Zahlen. Insofern sind zur Verschlüsselung nach Vigenère zunächst zu den Buchstaben des Schlüsselwortes am linken Streifen die zugehöri-

gen Schlüsselzahlen zu bestimmen. Zum Beispiel erhält man beim Schlüsselwort “Maus” die Zahlenfolge 12 0 19 17.

Verschlüsselt wird, indem der rechte Papierstreifen so weit gedreht wird, bis die jeweilige Schlüsselzahl dem zu verschlüsselnden Klartextbuchstaben gegenüberliegt. Der Pfeil auf dem rechten Papierstreifen zeigt nun auf das entsprechende Geheimtextzeichen. Beispielsweise erhält man bei der Schlüsselzahl 12 und dem zu verschlüsselnden Buchstaben S das Geheimtextzeichen E.

Die Entschlüsselung erfolgt entsprechend, indem man die Streifen so dreht, dass der Pfeil auf das jeweilige Geheimtextzeichen zeigt. Die Schlüsselzahl liegt nun in derselben Zeile wie der Klartextbuchstabe.

Auf dieselbe Weise kann man mit diesem Rotorgerät auch die später im Unterricht zu behandelnde Vernam–Chiffrierung mithilfe einer Folge von (zweistelligen) Zufallszahlen durchführen.

Daneben lässt sich an diesem Gerät auch die (bei asymmetrischen Chiffrierverfahren notwendige) Modulo–Rechnung gut veranschaulichen. Je nach Leistungsstand der Lerngruppe kann folglich bereits hier die Vigenère–Verschlüsselung mathematisch eingeführt werden. Mit dem i-ten Klartextbuchstaben k_i und dem i-ten Schlüsselbuchstaben s_i erhält man als Verschlüsselungsfunktion:

$$V(k_i) = (k_i + s_i) \bmod 25.$$

Anhang G

Berechnung des Schlüsselraums der Chiffriermaschine Enigma mit drei Schlüsselwalzen

Die Größe des Schlüsselraums setzt sich aus den Einstellungsmöglichkeiten der Enigma zusammen, d. h. aus

1. der Lage der Schlüsselwalzen,
2. der Stellung der Schlüsselwalzen,
3. der Ringstellung jeder Walze und
4. den Steckerverbindungen.

1. Lage der Schlüsselwalzen
Bei Auswahl der Lage bestehen für die erste Schlüsselwalze 3 Möglichkeiten; für die zweite gibt es 2 Möglichkeiten und für die dritte Schlüsselwalze bleibt nur noch eine Lage übrig. Damit erhält man

$$3! = 3 \cdot 2 \cdot 1 = 6$$

Möglichkeiten.

2. Stellung der Schlüsselwalzen
Jede Schlüsselwalze weist 26 Buchstaben und damit 26 verschiedene Stellungen auf. Bei drei Walzen erhält man folglich

$$26 \cdot 26 \cdot 26 = 17576$$

mögliche Einstellungen.

3. Ringstellung
Ein Ring weist 26 mögliche Stellungen auf, allerdings nur für die erste und die zweite Walze. Die Ringstellung der dritten Walze, die sich links vor der unbeweglichen Umkehrwalze befindet, ist bedeutungslos, da diese keine Walzen–Bewegung beeinflussen kann. Damit erhält man

$$26 \cdot 26 = 676$$

Einstellmöglichkeiten.

4. Steckerverbindungen
Für die Verbindung mit dem ersten Stecker gibt es zunächst 26 mögliche Buchstaben, für das Steckerende 25 Möglichkeiten. Damit erhält man $26 \cdot 25$ Auswahlmöglichkeiten. Da allerdings die Reihenfolge der Verkabelung keine Rolle spielt (es ist egal, ob z. B. A mit B oder B mit A verkabelt wird), entfällt die Hälfte der Möglichkeiten. Folglich erhält man für den ersten Stecker $\frac{26 \cdot 25}{2} = 325$ Wahlmöglichkeiten.

Für den zweiten Stecker hat man nun für den Steckeranfang 24 Buchstaben zur Verfügung, für das Steckerende noch 23. Analog ergeben sich hieraus $\frac{24 \cdot 23}{2} = 276$ Möglichkeiten.

Die Fortsetzung dieses Verfahrens liefert für sechs Stecker folgende Übersicht an Auswahlmöglichkeiten für den jeweiligen Stecker:

$$\begin{aligned}
&1.\ \text{Stecker } \tfrac{26\cdot 25}{2} = 325\\
&2.\ \text{Stecker } \tfrac{24\cdot 23}{2} = 276\\
&3.\ \text{Stecker } \tfrac{22\cdot 21}{2} = 231\\
&4.\ \text{Stecker } \tfrac{20\cdot 19}{2} = 190\\
&5.\ \text{Stecker } \tfrac{18\cdot 17}{2} = 153\\
&6.\ \text{Stecker } \tfrac{16\cdot 15}{2} = 120
\end{aligned}$$

Im Unterricht sollte dieses Verfahren auch auf den allgemeinen Fall übertragen werden. Stehen n Stecker zur Verfügung, gibt es für die Verkabelung des n-ten Steckers

$$\frac{1}{2}(26-(2n-2))\cdot(26-(2n-1))$$

Auswahlmöglichkeiten.

Die Gesamtzahl der Möglichkeiten für Steckerverbindungen liefert das Produkt der obigen Ergebnisse. Allerdings hat auch hier die Reihenfolge der Verkabelung keine kryptographischen Auswirkungen. So ist es gleichgültig, ob z. B. zuerst die Steckerverbindung A mit B und danach C mit D vorgenommen wird, oder umgekehrt. Bei 6 Steckern gibt es 6! verschiedene Reihenfolgen, die alle dasselbe kryptographische Ergebnis liefern. Folglich ist das erwähnte Produkt durch 6! zu dividieren. Insgesamt ergeben sich damit

$$\frac{1}{6!}\cdot 325\cdot 276\cdot 231\cdot 190\cdot 153\cdot 120 = 100391791500$$

Auswahlmöglichkeiten für die Steckerverbindungen.

Auch hier kann die Formel für den allgemeinen Fall mit n Steckern hergeleitet werden. Analog zu obigen Überlegungen erhält man

$$\frac{1}{n!}\prod_{i=1}^{n}\frac{(26-(2i-2))\cdot(26-(2i-1))}{2}$$

Auswahlmöglichkeiten für n Stecker.

Größe des Schlüsselraums
Die Zahl der möglichen Schlüssel ergibt sich aus der Multiplikation der einzelnen Teilergebnisse. Man erhält

$$7{,}156755733\cdot 10^{18}$$

mögliche Schlüssel.

Anhang H

Der ASCII–Code

Chr	Dez	Binär	Chr	Dez	Binär	Chr	Dez	Binär	Chr	Dez	Binär
NUL	0	00000000		32	00100000	@	64	01000000	’	96	01100000
SOH	1	00000001	!	33	00100001	A	65	01000001	a	97	01100001
STX	2	00000010	"	34	00100010	B	66	01000010	b	98	01100010
ETX	3	00000011	#	35	00100011	C	67	01000011	c	99	01100011
EOT	4	00000100	$	36	00100100	D	68	01000100	d	100	01100100
ENQ	5	00000101	%	37	00100101	E	69	01000101	e	101	01100101
ACK	6	00000110	&	38	00100110	F	70	01000110	f	102	01100110
BEL	7	00000111	’	39	00100111	G	71	01000111	g	103	01100111
BS	8	00001000	(	40	00101000	H	72	01001000	h	104	01101000
HT	9	00001001	)	41	00101001	I	73	01001001	i	105	01101001
LF	10	00001010	*	42	00101010	J	74	01001010	j	106	01101010
VT	11	00001011	+	43	00101011	K	75	01001011	k	107	01101011
FF	12	00001100	,	44	00101100	L	76	01001100	l	108	01101100
CR	13	00001101	-	45	00101101	M	77	01001101	m	109	01101101
SO	14	00001110	.	46	00101110	N	78	01001110	n	110	01101110
SI	15	00001111	/	47	00101111	O	79	01001111	o	111	01101111
DLE	16	00010000	0	48	00110000	P	80	01010000	p	112	01110000
DC1	17	00010001	1	49	00110001	Q	81	01010001	q	113	01110001
DC2	18	00010010	2	50	00110010	R	82	01010010	r	114	01110010
DC3	19	00010011	3	51	00110011	S	83	01010011	s	115	01110011
DC4	20	00010100	4	52	00110100	T	84	01010100	t	116	01110100
NAK	21	00010101	5	53	00110101	U	85	01010101	u	117	01110101
SYN	22	00010110	6	54	00110110	V	86	01010110	v	118	01110110
ETB	23	00010111	7	55	00110111	W	87	01010111	w	119	01110111
CAN	24	00011000	8	56	00111000	X	88	01011000	x	120	01111000
EM	25	00011001	9	57	00111001	Y	89	01011001	y	121	01111001
SUB	26	00011010	:	58	00111010	Z	90	01011010	z	122	01111010
ESC	27	00011011	;	59	00111011	[	91	01011011	{	123	01111011
FS	28	00011100	<	60	00111100	\	92	01011100	|	124	01111100
GS	29	00011101	=	61	00111101	]	93	01011101	}	125	01111101
RS	30	00011110	>	62	00111110	^	94	01011110	~	126	01111110
US	31	00011111	?	63	00111111	_	95	01011111	DEL	127	01111111

Anhang I

Schlüsselanzahl bei symmetrischen und asymmetrischen Chiffrierverfahren

Symmetrische Chiffrierverfahren
Die Anzahl der notwendigen Schlüssel in einem symmetrischen Kryptosystem lässt sich leicht anhand von Beispielen herleiten.

- Zwischen zwei Teilnehmern ist ein gemeinsamer Schlüssel zu vereinbaren.
- Zwischen drei Teilnehmern A, B und C ist ein Schlüssel zwischen A und B, ein Schlüssel zwischen A und C sowie ein Schlüssel zwischen B und C zu vereinbaren, damit jeder Kommunikationspartner mit jedem anderen vertrauliche Botschaften austauschen kann. Insgesamt sind damit 3 Schlüssel notwendig.
- Bei vier Teilnehmern A, B, C und D ist zwischen A und B, A und C, A und D, B und C, B und D sowie zwischen C und D jeweils ein Schlüssel zur vertraulichen Kommunikation auszutauschen. Insgesamt sind somit 6 Schlüssel vonnöten.
- Analog zeigt man, dass zwischen fünf Teilnehmern insgesamt 10 Schlüssel, zwischen sechs Teilnehmern 15 Schlüssel und zwischen sieben Teilnehmern 21 Schlüssel auszutauschen sind, wenn jeder mit jedem vertraulich kommunizieren möchte.

Trägt man die oben hergeleitete Schlüsselanzahl für die entsprechende Teilnehmerzahl in eine Tabelle ein, so erkennt man schnell, nach welcher Regel sich die Anzahl der Schlüssel entwickelt.

Anzahl der benötigten Schlüssel		
Anzahl der Teilnehmer	Anzahl der Schlüssel	Regel
2	1	
3	3	= 1 + 2
4	6	= 1 + 2 + 3
5	10	= 1 + 2 + 3 + 4
6	15	= 1 + 2 + 3 + 4 + 5
7	21	= 1 + 2 + 3 + 4 + 5 + 6

Analog sind für n Teilnehmer eines symmetrischen Kryptosystems

$$1 + 2 + 3 + ... + n - 1 = \frac{n(n-1)}{2}$$

Schlüssel notwendig.

Asymmetrische Chiffrierverfahren
Bei asymmetrischen Kryptosystemen ist für jeden Teilnehmer ein Schlüsselpaar, bestehend aus einem öffentlichen und einem geheimen Schlüssel notwendig, damit jeder Teilnehmer mit jedem anderen vertraulich kommunizieren kann. Bei n Teilnehmern sind folglich $2n$ Schlüssel vonnöten.

Literaturverzeichnis

[1] BATZER, P.: *Die Enigma*. LOG IN. Informatische Bildung und Computer in der Schule, 16:44 – 51, 1996.

[2] BAUER, F. L.: *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie*. Springer, Berlin, 2. Auflage, 2000.

[3] BAUMANN, R.: *Informationssicherheit durch kryptologische Verfahren*. LOG IN. Informatische Bildung und Computer in der Schule, 16:52 – 61, 1996.

[4] BAUMANN, R.: *Digitale Unterschrift*. LOG IN. Informatische Bildung und Computer in der Schule, 19:46 – 49, 1999.

[5] BECKER, K.-CL. und A. BEUTELSPACHER: *Datenverschlüsselung*. LOG IN. Informatische Bildung und Computer in der Schule, 16:16 – 21, 1996.

[6] BERLIN, J. und N. ROTH-SONNEN: *Von Cäsar zum Internet*. mathematik lehren, 129:15 – 20, 2005.

[7] BEUTELSPACHER, A.: *Mathe–Welt. Geheimschriften*. mathematik lehren, 72:23 – 46, 1995.

[8] BEUTELSPACHER, A.: *Kryptologie. Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen*. Vieweg, Braunschweig, 5. Auflage, 1996.

[9] BEUTELSPACHER, A., J. SCHWENK und K.-D. WOLFENSTETTER: *Moderne Verfahren der Kryptographie. Von RSA zu Zero-Knowledge*. Vieweg, Wiesbaden, 5. Auflage, 2004.

[10] BUCHMANN, J.: *Einführung in die Kryptographie*. Springer, Berlin, 3. Auflage, 2004.

[11] EPKENHANS, M.: *Die Kryptologie im Mathematikunterricht als Ideengeber für Facharbeitsthemen*. Mathematica Didactica, 25:17 – 36, 2002.

[12] GARFINKEL, SIMSON: *PGP. Pretty Good Privacy*. O'Reilly / International Thomson Verlag, Bonn, 1. Auflage, 1996.

[13] GÜNTHNER, H. und J. SCHMAILZL: *Kryptologie. Baustein zur Didaktik der Informatik*. Staatsinstitut für Schulpädagogik und Bildungsforschung, München, 1997.

[14] HERODOT: *Historien*. Heimeran Verlag, München, 1963.

[15] HORAK, H.: *Der bunte Zoo der Kryptologie*. Mathe–plus, 3, 1987.

[16] HTTP://HOME.IN.TUM.DE/∼GEROLD/AKTVORL2003/GLIEDERUNG.HTML.

[17] HUBWIESER, P.: *Didaktik der Informatik. Grundlagen, Konzepte, Beispiele*. Springer, Berlin, 2. Auflage, 2004.

[18] I. N. BRONSTEIN, K. A. SEMENDJAJEW, G. MUSIOL H. MÜHLIG: *Taschenbuch der Mathematik*. Verlag Harri Deutsch, Frankfurt am Main, 4. Auflage, 1999.

[19] JANK, W. und H. MEYER: *Didaktische Modelle*. Cornelson Scriptor, Frankfurt am Main, 1. Auflage, 1991.

[20] KIPPENHAHN, R.: *Verschlüsselte Botschaften. Geheimschrift, Enigma und Chipkarte*. Rowohlt Taschenbuch Verlag, Reinbek bei Hamburg, 4. Auflage, 2005.

[21] KIRSCH, CH.: *Unterschreibreform*. iX, 9:3, 2005.

[22] KLAFKI, W.: *Neue Studien zur Bildungstheorie und Didaktik. Zeitgemäße Allgemeinbildung und kritisch-konstruktive Didaktik*. Beltz, Weinheim, 3. Auflage, 1993.

[23] LEWIN, R.: *Entschied ULTRA den Krieg? Alliierte Funkaufklärung im 2. Weltkrieg*. Verlag Wehr & Wissen, Koblenz, 1981.

[24] MATTHEWS, R.: *A rotor device for periodic and random–key encryption*. Crytologia, XIII:266 – 272, 1989.

[25] MÜLLER-STACH, S.: *Drei Themen der Zahlentheorie*. MU - Der Mathematikunterricht, 5:4 – 13, 2006.

[26] PETERSSEN, W. H.: *Handbuch der Unterrichtsplanung. Grundfragen - Modelle - Stufen - Dimensionen*. Oldenbourg Schulbuchverlag, München, 9. Auflage, 2000.

[27] PLUTARCH: *Lebensbeschreibungen III*. Wilhelm Goldmann Verlag, München, 1964.

[28] POE, E. A.: *Grube und Pendel*. Insel Verlag, Frankfurt am Main, 2001.

[29] SCHULZ, R.-H.: *Primfaktorzerlegung*. LOG IN. Informatische Bildung und Computer in der Schule, 16:22 – 26, 1996.

[30] SING, S.: *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*. Deutscher Taschenbuch Verlag, München, 5. Auflage, 2004.

[31] STOHR, M. und K. BOLZ: *Konrad Zuse – Ein Visionär zwischen Null und Eins*. Netzwerkstatt Schule 3. Handlungsorientiertes Unterrichten mit Neuen Medien, Seiten 14 – 20, 2007.

[32] TRANQUILLUS, C. SUETONIUS: *Caesar*. Phillip Reclam jun., Stuttgart, 1999.

[33] VERNE, J.: *Reise zum Mittelpunkt der Erde*. A. Hartleben's Verlag, Wien, 1976.

[34] VERNE, J.: *Mathias Sandorf*. A. Hartleben's Verlag, Wien, 1979.

[35] WITTEN, H., I. LETZNER und R.-H. SCHULZ: *RSA & Co. in der Schule*. LOG IN. Informatische Bildung und Computer in der Schule, 18 - 19, 1998 - 1999.

[36] WOBST, REINHARD: *Abenteuer Kryptologie. Methoden, Risiken und Nutzen der Datenverschlüsselung*. Addison–Wesley Verlag, München, 3. Auflage, 2001.

[37] ZUBER, J.: *Kryptologie. Ein Wahlthema im Schuljahrgang 13*. LOG IN. Informatische Bildung und Computer in der Schule, 21:54 – 66, 2001.

Lebenslauf

Angaben zur Person

Name	Monika Stohr
Geburtsdatum	21.03.1979
Geburtsort	Kempten
Familienstand	verheiratet
Staatsangehörigkeit	deutsch

Werdegang

09.1985 – 07.1989	Grundschule Durach
09.1989 – 07.1998	Hildegardis–Gymnasium Kempten (Abschluss Allgemeine Hochschulreife)
11.1998 – 10.2002	Studium Lehramt Realschule für Mathematik und Wirtschaftswissenschaften an der Ludwig–Maximilians–Universität München (Abschluss der Ersten Staatsprüfung für das Lehramt an Realschulen)
10.2002 – 10.2003	Studium des Erweiterungsfaches Informatik an der TU München (Abschluss der Ersten Staatsprüfung als Erweiterungsprüfung im Fach Informatik)
02.2003 – 02.2005	Vorbereitungsdienst für das Lehramt an Realschulen (Abschluss der Zweiten Staatsprüfung)
seit 02.2005	Realschullehrerin an der Städtischen Elly–Heuss–Realschule in München