

M A S T E R A R B E I T

Elementare Kryptographie und ihre didaktische Umsetzung für die Schule

Elemental Cryptography and its Didactic Approach for School

Abgabedatum: 05.03.2014
Kerstin Bonfico
Matrikelnummer: 372057

Fachbereich Mathematik
unter Anleitung von
Prof. Dr. C. Fieker
Zweitkorrektor: H. Hürter

Inhaltsverzeichnis

Abbildungsverzeichnis V

Tabellenverzeichnis VII

1 Einleitung 1

2 Kryptographische Grundlagen 5
2.1 Verschlüsselungsverfahren . . . 5
2.2 Einführung in die Kryptoanalyse . . . 10
2.3 Perfekte Sicherheit . . . 11
2.4 Einführung in die Komplexitätstheorie . . . 13

3 Symmetrische Verschlüsselungsverfahren 17
3.1 Die Skytala von Sparta . . . 17
3.2 Die Caesar-Verschlüsselung . . . 20
3.3 Die Vigenère-Verschlüsselung . . . 24
3.3.1 Der Kasiski-Test . . . 27
3.3.2 Der Friedmann-Test . . . 27

4 Public-Key-Verfahren 31
4.1 Das RSA-Verfahren . . . 31
4.1.1 Der Algorithmus . . . 31
4.1.2 Sicherheit . . . 34
4.1.2.1 Faktorisierungsangriffe . . . 35
4.1.2.2 Weitere Angriffsmöglichkeiten . . . 40
4.1.2.3 Parameter-Empfehlungen . . . 41
4.2 Der Diffie-Hellman-Schlüsselaustausch . . . 42
4.2.1 Der diskrete Logarithmus . . . 42
4.2.2 Schlüsselaustausch . . . 43
4.2.3 Sicherheit . . . 44
4.2.3.1 Enumeration . . . 45
4.2.3.2 Babystep-Giantstep-Algorithmus . . . 45

5 Planung der Unterrichtsreihe 47
5.1 Lehrplan und Bildungsstandards . . . 47
5.2 Ziele der Unterrichtsreihe . . . 48
5.3 Bedeutung des Unterrichtsgegenstandes Kryptographie . . . 49

5.4 Mögliches Vorwissen aus dem Fach Informatik 50
5.5 Analyse der Themenkomplexe 51
5.6 Tabellarische Reihenplanung 54

6 Unterrichtsentwürfe **57**
6.1 Einführung & Verschlüsselungsverfahren 57
6.2 Perfekte Sicherheit 69
6.3 Diffie-Hellman-Schlüsselaustausch 79

7 Fazit **91**

Literaturverzeichnis **XII**

Anhang **XIII**
A Mathematische Grundlagen XIII
A1 Stochastik XIII
A2 Zahlentheorie XIV
B Klartext des Beispiels zur Vigenère-Verschlüsselung XVII
C Unterrichtsmaterial XVIII

Abbildungsverzeichnis

1.1 Alice, Bob und Eve 2

2.1 Das Prinzip des Public-Key-Verfahrens 7
2.2 Schematische Darstellung einer Blockchiffre 8
2.3 Funktionsweise des One-Time-Pad 9

3.1 Skytala von Sparta 17
3.2 Die Caesar-Scheibe 21
3.3 Das Vigenère-Quadrat 24

4.1 Man-in-the-Middle Angriff 41
4.2 Diffie-Hellman-Schlüsselaustausch: Kommunikationsbeispiel 44

5.1 Auszug aus dem Lehrplan Informatik 50

6.1 Fragensammlung 60
6.2 Verschlüsselungsmaschinen 64
6.3 Rechnen modulo 26 65
6.4 Beweispuzzle 72
6.5 Abreißblock zur Veranschaulichung des One-Time-Pads 83
6.6 Schlüssel-Schloss Modell zur Veranschaulichung des Diffie-Hellman Schlüsselaustausches 83

Tabellenverzeichnis

2.1 Vergleich einiger Polynomial- und Exponentialfunktionen 15

3.1 Die Häufigkeiten der Buchstaben in deutschen Texten 22
3.2 Eine homophone Chiffrierung 23

4.1 Beispiel: Quadratisches Sieb 38

5.1 Unterrichtsreihenplanung 54

6.1 Tabellarischer Verlaufsplan Einheit 1 66
6.2 Tabellarischer Verlaufsplan Einheit 2 75
6.3 Tabellarischer Verlaufsplan Einheit 3 85

»Cryptography is a charming and rewarding way to introduce into the classroom subjects of traditional mathematics, algebra, modular arithmetic, computational linguistic, combinatorics, algorithms,. . . «

- Massimo Borelli [15], S.2

1 Einleitung

Kryptographie ist, ihrer Wortherkunft nach, die Wissenschaft von der Verschlüsselung von Informationen (altgr. $\kappa\rho\upsilon\pi\tau o\sigma$ für geheim, $\gamma\rho\alpha\varphi\epsilon\iota\nu$ für schreiben). Zusammen mit der **Kryptoanalyse** bildet sie die Wissenschaft der **Kryptologie**[3]. Ziel der Kryptoanalyse ist es, Informationen aus verschlüsselten Nachrichten zu gewinnen. Heute werden die Begriffe Kryptographie und Kryptologie oft synomym benutzt, denn die Entwicklung von Verschlüsselungssystemen bindet unweigerlich Überlegungen zur Kryptoanalyse mit ein: Soll ein System als sicher gelten, müssen vorher mögliche Angriffe auf das System überprüft werden.

Die Kryptographie ist eine sehr alte Wissenschaft. Das erste überlieferte Verschlüsselungssystem, die Skytala von Sparta, wurde schon vor mehr als 2500 Jahren genutzt. Bis heute wurden unzählige Systeme entwickelt und verbessert. Sie spielen z. B. bei der Übermittlung von Daten im Internet, bei Geldüberweisungen oder bei der Nutzung von Chipkarten eine große Rolle. Die Wichtigkeit der Kryptographie in der heutigen Zeit wird durch folgendes Zitat deutlich:

> „ *Starke Kryptografie kann jeder noch so großen Gewalt widerstehen. Keine Ballung von Zwang und Macht kann jemals das mathematische Problem lösen.* “ -Julian Assange, Sprecher der Enthüllungsplattform WikiLeaks, [5] Absatz 3.

Assange bezeichnet damit die Kryptographie als „einzige Hoffnung gegen die totale Dominanz des Überwachungsstaates“ ([5] Absatz 3) und nimmt gleichzeitig Bezug auf die faszinierende Rolle der Mathematik innerhalb der Kryptographie.

Die Ziele der Kryptographie reichen heute weit über das bloße Verschlüsseln einer Nachricht hinaus. Folgenden drei Grundproblemen widmet sich diese Wissenschaft (Beueltspacher 2010, [4]):

- **Geheimhaltung:** Eine Nachricht soll an einen Empfänger versendet werden, ohne dass mögliche Angreifer die Nachricht lesen oder abhören können. Die Nachricht wird dabei so verändert (verschlüsselt), sodass sie zunächst unkenntlich gemacht, aber für den Empfänger leicht zu Entschlüsseln ist. Dieser muss also im Besitz eines weiteren Geheimnisses, des Schlüssels, sein.
- **Authentikation:** Wenn ein Empfänger eine Nachricht erhält, wie kann er sich dann sicher sein, dass die Nachricht vom angegebenen Sender stammt und nicht verändert wurde? Man spricht in diesen Fällen von der *Teilnehmerauthentikation* und der *Nachrichtenauthentikation*. Der Sender kann seine

Identität z. B. durch Angabe eines Passwortes oder einer Geheimzahl, etwa am Geldautomaten, nachweisen. Im zweiten Fall muss der Sender die Nachricht so gestalten, dass dem Empfänger eine Veränderung durch eine dritte Person auffallen würde.

- **Anonymität:** In manchen Situationen, etwa bei der Kommunikation im Internet, sollen die beteiligten Personen anonym bleiben. Man spricht von *Sender- und Empfängeranonymität.*

Diese Arbeit wird sich vorrangig mit dem Problem der Geheimhaltung befassen. Dazu werden an dieser Stelle drei Hauptcharaktere eingeführt: Alice, Bob und Eve. Wie Abbildung 1.1 zeigt, möchte Alice eine Nachricht an Bob schicken. Eve ist eine Angreiferin, die die Nachricht mitzuhören versucht[1] .



Abbildung 1.1: Alice, Bob und Eve, Quelle: Eigene Darstellung

In dieser Arbeit soll Kryptographie als spannendes und bedeutsames Anwendungsfeld der Mathematik im Hinblick auf eine **Einbindung in den Schulunterricht** der Oberstufe betrachtet werden. Massimo Borelli vom Department of Mathematical Sciences der University of Trieste beschreibt das Potential der Kryptographie im Schulunterricht wie folgt:

> „*Cryptography is a charming and rewarding way to introduce into the classroom subjects of traditional mathematics, algebra, modular arithmetic, computational linguistic, combinatorics, algorithms,...*“[15], S.2

Bestandteil dieser Arbeit ist es also, eine Unterrichtsreihe zum Thema Kryptographie zu entwickeln. Dazu werden zunächst grundlegende Verschlüsselungssysteme beschrieben und hinsichtlich ihrer Sicherheit untersucht. In Kapitel 2 werden hierfür kryptographische Grundlagen bereitgestellt. Es wird geklärt, was genau unter einem Verschlüsselungssystem zu verstehen ist, wann man dieses als sicher bezeichnen kann und welche Angriffe auf solche Systeme unterschieden werden.

[1] Oft wird zwischen der passiven Angreiferin Eve und aktiven Angreifern (Mallory oder Oskar) unterschieden. In dieser Arbeit werden sowohl passive als auch aktive Angreifer durch Eve verkörpert.

Die folgenden beiden Kapitel beschreiben verschiedene Verschlüsselungssysteme, angefangen in Kapitel 3 bei einfachen und sehr alten Systemen wie der Skytala von Sparta, der Caesar- und der Vigenère-Verschlüsselung. Kapitel 4 befasst sich mit modernen Verfahren, wie dem RSA-Algorithmus und dem Diffie-Hellman Schlüsselaustausch.
Kapitel 5 befasst sich mit der schulischen Einbindung der Kryptographie. Es wird eine Unterrichtsreihe für einen Leistungskurs der Oberstufe erarbeitet, welche, über interessante Grundlagen hinaus, Einblicke in das Mathematikstudium ermöglichen soll. Die Reihe ist für die Zeit nach dem schriftlichen Abitur konzipiert. Sie soll zum einen einen spannenden und motivierenden Unterricht ermöglichen und zum anderen eine Orientierungshilfe zur Studienwahl darstellen.
In Kapitel 6 werden die einzelnen Unterrichtsstunden anhand von Unterrichtsentwürfen beschrieben. Neben einer ausführlichen didaktischen und methodischen Analyse werden tabellarische Unterrichtsentwürfe und die benötigten Materialien bereit gestellt.

2 Kryptographische Grundlagen

In diesem Kapitel werden die Grundlagen, die zum Verständnis der in Kapitel 3 und 4 vorgestellten Verschlüsselungsverfahren benötigt werden, erläutert. Der Begriff des Verschlüsselungsverfahrens wird konkretisiert und ein erster Einstieg in die Kryptoanalyse erfolgt. Im Anschluss wird die Frage geklärt, welche Bedingungen ein Verschlüsselungsverfahren erfüllen muss, um als sicher zu gelten. Abschließend wird ein kurzer Einblick in die Komplexitätstheorie gegeben.

2.1 Verschlüsselungsverfahren

Verschlüsselungsverfahren oder *Kryptosysteme* dienen dazu, Nachrichten zu verschlüsseln, also deren Inhalt für nicht befugte Leser unkenntlich zu machen. Im Folgenden werden Definitionen und Begriffe eingeführt, mit deren Hilfe solche Verfahren näher beschrieben und klassifiziert werden können.
Dieses Kapitel beruht weitestgehend auf Buchmann, [7], Kapitel 3.

Eine Nachricht, ein Passwort oder eine Geheimzahl bestehen jeweils aus einer Aneinanderreihung von Zeichen, welche aus einer gemeinsamen Grundmenge, dem Alphabet, stammen.

Definition 2.1.1. Ein *Alphabet* A ist eine endliche, nichtleere Menge. Es gilt:

(i) Die Elemente aus A heißen Buchstaben. $|A|$ ist die Anzahl der Buchstaben im Alphabet.

(ii) Ein Element $w = (\omega_1, \ldots, \omega_l) \in A^l$, $l \in \mathbb{N}$ heißt Wort der Länge l.

(iii) Die Menge $A^* = \bigcup_0^\infty A^l$ enthält alle Wörter oder Texte beliebiger Länge.

Beispiel 2.1.2.

(i) $A = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z\}$
Das uns bekannte natürliche Alphabet hat die Länge $|A| = 26$. Die Menge A^* enthält alle Aneinanderreihungen von Buchstaben in beliebiger Reihenfolge und Länge. Die Menge der sinnvollen deutschen Texte ist wesentlich kleiner und eine Untermenge von A^*.

(ii) Das in der Datenverarbeitung genutzte Alphabet $A = \{0, 1\}$ hat die Länge $|A| = 2$. Die Elemente aus A^* werden Bitfolgen genannt.

Nun ist es möglich, den Begriff des Verschlüsselungsverfahrens zu definieren.

Definition 2.1.3. Seien A und B Alphabete. Ein *Verschlüsselungsverfahren* ist ein Fünftupel (M, C, K, E, D)[1] mit folgenden Eigenschaften:

(i) $M \subseteq A^*$ heißt Klartextraum. Die Elemente aus M heißen Klartexte oder Nachrichten.

(ii) $C \subseteq B^*$ heißt Geheimtextraum. Die Elemente aus C heißen Geheimtexte.

(iii) K ist eine Menge. Sie heißt Schlüsselraum. Ihre Elemente heißen Schlüssel.

(iv) $E = \{E_k : k \in K\}$ ist eine Familie von Funktionen $E_k : M \to C$. Ihre Elemente heißen Verschlüsselungsfunktionen.

(v) $D = \{D_k : k \in K\}$ ist eine Familie von Funktionen $D_k : C \to M$. Ihre Elemente heißen Entschlüsselungsfunktionen.

(vi) Für jedes $e \in K$ gibt es ein $d \in K$, sodass für alle $m \in M$ die Gleichung

$$D_d(E_e(m)) = m$$

gilt.

Bemerkung 2.1.4.

(i) In dieser Definition stammen die Schlüssel e und d aus der gleichen Schlüsselmenge K. Oft spricht man auch von zwei Schlüsselmengen: Der Menge der Schlüssel K und der Menge der Entschlüsselungsschlüssel $\overline{K}$.

(ii) Um eine eindeutige Entschlüsselung zu gewährleisten, gilt: $|C| \geq |M|$.

Für die Kommunikation zwischen Alice und Bob ergeben sich folgende Konsequenzen [23], S.7f:

- Alice und Bob müssen sich auf ein Verschlüsselungsverfahren einigen. Das zugrundeliegende Alphabet, die Ver- und Entschlüsselungsfunktionen (der Algorithmus) sowie die Schlüsselmenge müssen beiden bekannt sein.

- Vor der Versendung der Nachricht müssen sich Bob und Alice auf ein Schlüsselpaar (e, d) einigen. Man spricht hierbei vom Schlüsselaustausch. Auch an dieser Stelle besteht das Problem den Schlüsselaustausch so sicher wie möglich zu gestalten. Da der Schlüssel aber meist viel kleiner als die eigentliche Nachricht ist, kann der Tausch auf langsamen, aber sicheren Wegen erfolgen. Alice kann z. B. ein Treffen mit Bob vereinbaren, um die Schlüssel festzulegen. Dieses Treffen kann zu jedem beliebigen Zeitpunkt stattfinden. Die Nachrichtenübermittlung kann im Nachhinein relativ spontan und über schnellere Wege, wie z. B. über E-mail erfolgen.

Im Folgenden werden drei Kategorisierungen vorgestellt, in die Verschlüsselungssysteme eingeordnet werden können.

[1] Die Großbuchstaben entstammen den englischen Bezeichnungen Messagespace, Ciphertextspace, Keyspace, Encryption und Decryption.

Symmetrische und Asymmetrische Verschlüsselung

Wird zum Ver- und Entschlüsseln der gleiche Schlüssel ($e = d$) benutzt oder lässt sich d leicht aus e berechnen, so heißt das Verfahren *symmetrisch*. Ist allerdings d nicht mit angemessenem Aufwand aus e zu berechnen, so nennt man das Verfahren *asymmetrisch*. In diesem Fall veröffentlicht Bob einen öffentlichen Schlüssel e, aber hält seinen Schlüssel d geheim. Alice kann nun e zum Verschlüsseln benutzen (siehe Abb.2.1).

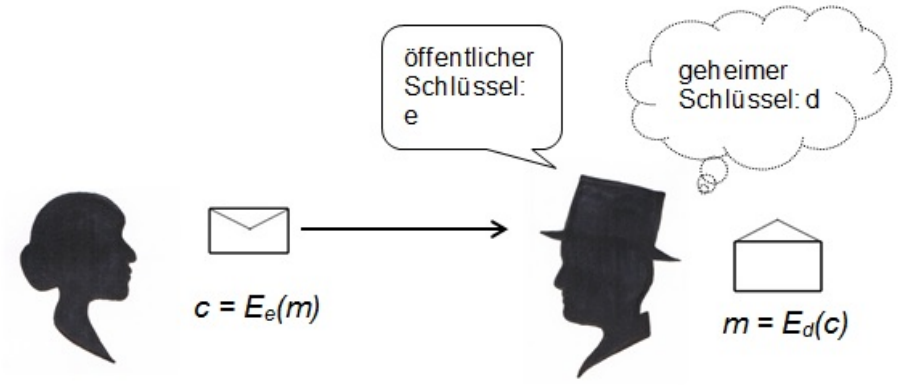


Abbildung 2.1: Das Prinzip des Public-Key-Verfahrens, Quelle: Eigene Darstellung

Nur Bob kann die Nachricht mit seinem geheimen Schlüssel d entschlüsseln. Solche Verfahren werden auch als *Public-Key-Verfahren* bezeichnet. Das bekannteste solcher Verfahren, der RSA-Algorithmus, wird in Kapitel 4 näher beschrieben.

Transpositions- und Substitutionsverfahren

Bei einem *Transpositionsverfahren* werden die Buchstaben des Klartextes permutiert, d. h. die Buchstaben bleiben gleich, tauschen aber ihre Plätze. Im Gegensatz dazu verhält sich das *Substitutionsverfahren*: Die Klartextbuchstaben behalten zwar ihre Position, werden aber durch einen Geheimtextbuchstaben ersetzt. Innerhalb der Substitutionsverfahren unterscheidet man weiterhin zwischen **monoalphabetischen** und **polyalphabetischen** Verfahren: Bei einem *monoalphabetischen* Verfahren wird ein Klartextbuchstabe immer durch denselben Geheimtextbuchstaben substituiert. Beim *polyalphabetischen* Verfahren können mehrere Geheimtextbuchstaben den gleichen Klartextbuchstaben repräsentieren, [8].

Ein sehr allgemein formuliertes Substitutionsverfahren ist das affin lineare Verfahren:

Definition 2.1.5. Sei $m, l \in \mathbb{N}$ und $A = B = \mathbb{Z}_m$, wobei $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$. Dann ist (M, C, K, E, D) ein *affin lineares Verschlüsselungssystem*, wenn gilt:

(i) $M = C = A^l$

(ii) $K = \{(a, b) \mid a \in (\mathbb{Z}/m\mathbb{Z})^{l \times l}, b \in (\mathbb{Z}/m\mathbb{Z})^l, \text{ggt}(\det(a), m) = 1\}$

(iii) $E_k : M \to C,\ x \mapsto ax + b \bmod m$ für $k = (a, b),\ x \in M$

(iv) $D_{k'} : C \to M, x \mapsto a'(x-b) \bmod m$ für $k' = (a', b), x \in C$ mit $a' \cdot a \equiv 1 \bmod m$

(v) Es gilt: $\begin{aligned} D_{k'}(E_k(x)) &= a'((ax + b \bmod m) - b) \bmod m \\ &= a'(ax + b - b) \bmod m \\ &= a'ax = x \bmod m \end{aligned}$

Betrachten wir die einzelnen Buchstaben eines Klartextes $x \in M$, so ist dieses Verfahren für $l > 1$ polyalphabetisch: Taucht im Klartext ein Buchstabe mehrmals auf, so wird er im Allgemeinen durch verschiedene Geheimtextbuchstaben ersetzt. Für $l = 1$ ergibt sich ein monoalphabetisches Verfahren[2]. Beispiele affin linearer Verfahren werden in Kapitel 3 vorgestellt. Es wird sich zeigen, dass diese relativ einfach zu entschlüsseln sind.

Block- und Stromchiffren

Dieser Abschnitt ist an Beutelspacher [4], Kapitel 2 angelehnt.
Bei einer *Blockchiffre* wird die Nachricht in Blöcke fester Länge unterteilt (siehe Abb. 2.2):

$$m = (m_1, m_2, m_3, ...).$$

Die Verschlüsselungsfunktion wird dann auf die einzelnen Blöcke angewendet:

$$c_i = E_k(m_i).$$

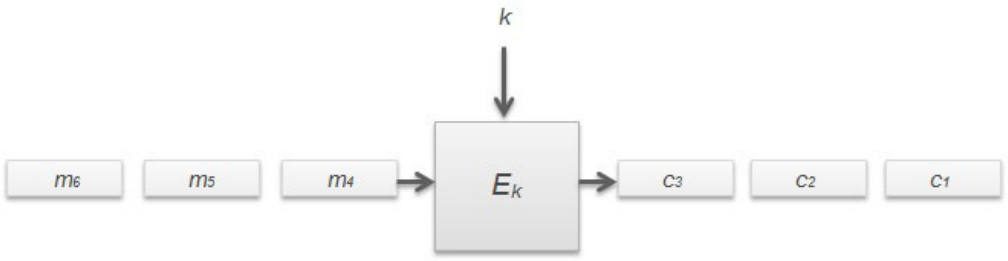


Abbildung 2.2: Schematische Darstellung einer Blockchiffre, Quelle: Eigene Darstellung nach [4], S.8)

[2] Betrachtet man die Verschlüsselung von ganzen Wörtern oder Texten der Länge l, so ist die Verschlüsselung für alle l monoalphabetisch: Gleiche Wörter oder Texte werden auf gleiche Art und Weise verschlüsselt.

Die *Stromchiffre* hingegen verschlüsselt die Nachricht mithilfe eines Schlüsselstroms zeichenweise. Im Gegensatz zur Blockchiffre, bei der nur ein Schlüssel für alle Blöcke verwendet wird, werden hier im Allgemeinen gleiche Klartextbuchstaben in unterschiedliche Geheimtextbuchstaben verschlüsselt. Eines der ersten entwickelten Stromchriffren ist das *One-Time-Pad*. Abbildung 2.3 zeigt die Funktionsweise anhand eines Beispiels.



Abbildung 2.3: Funktionsweise des One-Time-Pad, Quelle: Eigene Darstellung nach [4], S.9

Definition 2.1.6. Das One-Time-Pad
Das *One-Time-Pad* wird mit Bits betrieben. Für $A = \{0, 1\}$ gilt:

(i) $M = C = K = A^l$ enthalten alle Bitfolgen der Länge l.

(ii) $E_k : M \to C$ mit $k = (k_1, \ldots, k_l)$, $m = (m_1, \ldots, m_l)$ und $c = (c_1, \ldots, c_l)$ operiert durch binäre Addition:

$$m_i \mapsto m_i \oplus k_i, \quad i = 1, 2, \ldots, l$$

wobei gilt: $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$

(iii) $E_k = D_k$, d. h. entschlüsselt wird durch erneute Addition des Schlüsselstroms.

(iv) Es gilt: $D_k(E_k(m_i)) = (m_i \oplus k_i) \oplus k_i = m_i \oplus (k_i \oplus k_i) = m_i \oplus 0 = m_i$

Der Schlüssel muss beim *One-Time-Pad* genauso lang sein wie der Klartext. Wird der Schlüssel nur einmal verwendet und handelt es sich dabei um eine echte Zufallsbitfolge, bei welcher die Werte 0 und 1 mit gleicher Wahrscheinlichkeit auftreten, so ist dies ein *perfekt sicheres* Verfahren (siehe Abschnitt 2.3), welches aber bei großen Texten sehr uneffizient und damit für die Praxis sehr ungeeignet ist. Man verwendet stattdessen oft Pseudozufallsgeneratoren, die aus einer kurzen Initialisierungs-Bitfolge einen pseudo-zufälligen Schlüssel generieren. Die Schlüsselübertragung wird dadurch erleichtert, das System ist allerdings nicht mehr uneingeschränkt sicher. Seinen Namen hat das System von der Vorstellung eines Abreißblocks: Auf jedem Blatt steht ein Schlüsselbit und wird, nach dessen Verwendung, abgerissen.

2.2 Einführung in die Kryptoanalyse

Als Vorlage für diesen Abschnitt dienen die Bücher von Beutelspacher, [4] und [3]. Wie schon in Abschnitt 2.1 beschrieben, führen Alice und Bob vor dem Nachrichtenaustausch einen Schlüsselaustausch durch. Die Geheimhaltung des Schlüssels steht dabei im Vordergrund. Kerkhoff formulierte dies 1883 erstmals in *La cryptographie militaire*. Die Kernaussage wird heute als Kerkhoffsches Prinzip bezeichnet.

Kerkhoffsches Prinzip
Die Sicherheit eines Kryptosystems hängt nicht von der Geheimhaltung des Algorithmus ab, sondern beruht nur auf der Geheimhaltung des Schlüssels.

In der Tat beruht die moderne Kryptographie auf diesem Prinzip. Ein Algorithmus gilt oft erst dann als sicher, wenn er eine Zeit lang der Diskussion in der Öffentlichkeit stand gehalten hat. Der AES-Algorithmus ist sogar im Zuge einer öffentlichen Ausschreibung entstanden.

Angriffsszenarien auf Verschlüsselungssysteme

Nicht immer liegt der Angreiferin Eve nur der Geheimtext vor. Es ist z. B. auch denkbar, dass sie ein Stück vom Klartext oder den Algorithmus (also Ver- und Entschlüsselungsfunktionen) kennt. Im Folgenden werden mögliche Angriffe skizziert, welche sich in den Informationen, die der Angreifer über Geheimtext, Schlüsseltext und Algorithmus hat, unterscheiden.

- *Known ciphertext attack:* Eve hat eine Nachricht abgefangen und kennt ein relativ großes Stück vom Geheimtext. Sie versucht daraus Rückschlüsse auf den verwendeten Algorithmus, den Schlüssel und damit den Klartext zu ziehen.
- *Known plaintext attack:* In diesem Fall liegt Eve, zusätzlich zu einem kleinen Stück Geheimtext, der zugehörige Klartext vor. Dies ist z. B. denkbar, wenn Eve die üblich genutzten Begrüßungsfloskeln kennt.
- *Chosen plaintext attack:* Eve hat Zugang zur Verschlüsselungsfunktion E_k. Sie kennt zwar die Schlüssel nicht, kann den aktuellen Schlüssel k aber benutzen. Sie verschlüsselt selbst gewählte Klartexte. Diese wählt sie möglichst einfach, z. B. $m = aaaa$, um dann aus dem erhaltenen Geheimtext Rückschlüsse auf E_k und k ziehen zu können. Hier besteht die Gefahr, dass Eve unbemerkt einen zu Alices ähnlichen, aber in wesentlichen Merkmalen veränderten, Klartext verschlüsselt und an Bob verschickt.
- *Chosen ciphertext attack:* In diesem Fall hat Eve Zugang zur Entschlüsselungsfunktion D_k mit dem aktuellen Schlüssel k. Sie entschlüsselt selbst gewählte Texte und versucht mithilfe der zugehörigen Klartexte k zu berechnen.

Die Methoden der Kryptoanalyse hängen stark von den verwendeten Verschlüsselungssystemen und deren Eigenschaften ab. Sie werden in den Kapiteln 3 und 4

näher erläutert. Ein sehr effektives aber oft zeitaufwendiges Verfahren sei an dieser Stelle schon genannt: Die *Brute-Force Methode* oder *Exhaustive Key Search*. Dabei testet Eve alle möglichen Schlüssel systematisch. Sie wird im Schnitt nach $|K|/2$ Versuchen auf den richtigen Schlüssel stoßen. Im aufwändigsten Fall benötigt sie $|K|$ Versuche zum Entschlüsseln des Textes.

2.3 Perfekte Sicherheit

In Abschnitt 2.1 wurde schon ein perfekt sicheres Verfahren vorgestellt: Das One-Time-Pad. Doch was genau versteht man unter *perfekter Sicherheit*? Intuitiv würde man sagen, damit ein System als sicher gilt, darf Eve keinerlei Chance haben, ihre Informationen über das System zu vergrößern. Dieser Gedanke soll im Folgenden formalisiert werden (angelehnt an [20], Abschnitt 4.3).

Bemerkung 2.3.1. Eve nutzt das Verschlüsselungsverfahren (M, C, K, E, D) mit endlichem Klartext-, Geheimtext- und Schlüsselraum und $|C| \geq |M|$. Für das Auftreten der Klartexte, Geheimtexte und Schlüssel werden folgende Wahrscheinlichkeitsverteilungen angenommen[3]:

(i) $P_M : M \to [0,1]$ mit $m \mapsto P_M(m)$ ist die a-priori-Wahrscheinlichkeit für das Auftreten des Klartextes $m \in M$. Sie ist meist abhängig von der verwendeten Sprache.

(ii) $P_K : K \to [0,1]$ mit $k \mapsto P_K(k)$ ist die a-priori-Wahrscheinlichkeit für das Auftreten des Schlüssels $k \in K$. Es gilt $P_K(k) > 0$ für alle $k \in K$.

(iii) $P_{M\times K} : (M \times K) \to [0,1]$ mit $(m,k) \mapsto P_{M\times K}(m,k)$ ist die Wahrscheinlichkeit dafür, dass der Klartext $m \in M$ vom Schlüssel $k \in K$ verschlüsselt wurde. Es gilt:

$$P_{M\times K}(m,k) = P_M(m) \cdot P_K(k)$$

Die Ereignisse m und k sind also unabhängig.

(iv) Für die Wahrscheinlichkeit $P_C : C \to [0,1]$ mit $c \mapsto P_C(c)$ für das Auftreten des Schlüsseltextes $c = E_k(m)$ gilt:

$$P_C(c) = \sum_{(m,k):\ E_k(m)=c} P_{M\times K}(m,k)$$

Eve kann nur dann Rückschlüsse auf den Klartext ziehen, falls der Geheimtext manche Klartexte wahrscheinlicher macht als andere. Dies führt zu folgender Definition:

[3] Die zugrundeliegenden stochastischen Definitionen sind im Anhang A1 nachzulesen.

Definition 2.3.2. Ein Verschlüsselungsverfahren heißt *perfekt sicher*, wenn die Wahrscheinlichkeit eines Klartextes nicht vom vorliegenden Geheimtext abhängt:

$$P(m|c) = P_M(m)$$

d.h. wenn die a-posteriori-Wahrscheinlichkeit einer Nachricht gleich ihrer a-priori-Wahrscheinlichkeit ist.

Beispiel 2.3.3. Sei (M, C, K, E, D) ein Verschlüsselungssystem mit

- $M = \{a, b\}$: $P_M(a) = 0,25$ und $P_M(b) = 0,75$
- $C = \{1, 2, 3, 4\}$
- $K = \{e_1, e_2, e_3, e_4\}$:
  $P_K(e_1) = 0,2$; $P_K(e_2) = 0,5$; $P_K(e_3) = 0,2$ und $P_K(e_4) = 0,1$

Die Ver- und Entschlüsselung ist durch folgende Zuordnungstabelle gegeben:

	e_1	e_2	e_3	e_4
a	1	2	3	4
b	4	1	2	3

Falls nun z. B. $c = 1$, dann müsste, im Falle eines perfekt sicheren Systems, die Wahrscheinlichkeit, dass der zugehörige Klartext a ist, gleich der a-priori-Wahrscheinlichkeit von a sein. Es ist aber:

$$P(a|1) = \frac{P(a,1)}{P_C(1)} = \frac{P(a,e_1)}{P(a,e_1) + P(b,e_2)} = \frac{0,25 \cdot 0,2}{0,25 \cdot 0,2 + 0,75 \cdot 0,5} = \frac{0,05}{0,425} \approx 0,12 \neq P_M(a)$$

und damit ist das Verfahren nicht perfekt sicher.

Satz 2.3.4. Satz von Shannon
Sei $|C| = |K|$ und $P_M(m) > 0$ für alle $m \in M$. Das Verschlüsselungsverfahren ist genau dann perfekt sicher, wenn gilt:

(i) P_K ist die Gleichverteilung und

(ii) für alle $m \in M$ und für alle $c \in C$ existiert genau ein $k \in K$ mit: $c = E_k(m)$.

Beweis:
„⇒“ Das Verfahren sei perfekt sicher. Sei $m \in M$. Falls ein $c \in C$ existiert, für das es kein $k \in K$ gibt mit $c = E_k(m)$ dann ist $P(m|c) = 0$. Nach Voraussetzung ist aber $P_M(m) > 0$, also: $P(m|c) \neq P_M(m)$ im Widerspruch zur perfekten Sicherheit des Systems. Es folgt daher: Für alle $c \in C$ existiert ein k mit $E_k(m) = c$. Da außerdem $|C| = |K|$ ist, gibt es immer genau einen Schlüssel.

Sei nun $c \in C$ beliebig aber fest. Für $m \in M$ sei k_m der Schlüssel für den gilt: $E_{k_m}(m) = c$. Es ist:

$$P_M(m) = P(m|c) = \frac{P(c|m)P_M(m)}{P_C(c)} = \frac{P(k_m)P_M(m)}{P_C(c)}$$

Es gilt also $P(k_m) = P_C(c)$ unabhängig von m. Die Wahrscheinlichkeiten für die Schlüssel sind also alle gleich: $P_K(k) = \frac{1}{|K|}$ und damit ist P_K die Gleichverteilung.
„$\Leftarrow$“ Es gilt:

$$\begin{aligned} P(m|c) &= \frac{P_M(m)P(c|m)}{P_C(c)} = \frac{P_M(m)P_K(k_{m,c})}{\sum_{n \in M} P_M(n)P_K(k_{n,c})} \\ &= \frac{P_M(m)P_K(k_{m,c})}{\sum_{n \in M} P_M(n)\frac{1}{|K|}} = \frac{P_M(m)P_K(k_{m,c})}{\frac{1}{|K|}} \end{aligned}$$

Da $P_K(k_{m,c}) = \frac{1}{|K|}$ für alle $k \in K$ ist $P(m|c) = P_M(m)$ und damit gilt das Verfahren als perfekt sicher. □

Bemerkung 2.3.5. Aus diesem Satz folgt:

- Das Verschlüsselungsverfahren aus Beispiel 2.3.3 wäre perfekt sicher, falls gilt: $P_K(e_i) = 0,25$ für alle i .
- Das One-Time-Pad ist perfekt sicher, da $|C| = |K| = \{0,1\}^n$, $P_K(0) = P_K(1) = 0,5$ und die Bedingung in Satz 2.3.2 *ii)* durch die binäre Addition gegeben ist.

2.4 Einführung in die Komplexitätstheorie

Um Verschlüsselungsverfahren hinsichtlich ihrer Effizienz beurteilen zu können, müssen zunächst Aussagen über den benötigten Aufwand, also ihre Komplexität, getroffen werden. Dieser Abschnitt gibt lediglich einen kurzen Einblick in die Komplexitätstheorie. Die Inhalte können vertieft in Rothe, [20], Kapitel 3 nachgelesen werden.
Einem zu lösenden Problem wird eine Berechnungskomplexität in Abhängigkeit der verwendeten Geräte / des Algorithmus zugewiesen. Es wird dabei unterschieden in:

- **Die Zeitkomplexität** als Anzahl der benötigten Schritte eines Algorithmus bei einer gegebenen Eingabe.
- **Die Raumkomplexität** als benötigter Speicherplatz bei gegebener Eingabe.

Die Angabe der Komplexität erfolgt jeweils durch Komplexitätsfunktionen, welche in Abhängigkeit von der Eingabegröße dargestellt werden. Dabei wird meist als Wert für die Funktion für einen Algorithmus und eine Eingabegröße n die maximal mögliche Komplexität verwendet (*Worst Case Komplexität)*. Um solche Abschätzungen zu vereinfachen, bedient man sich der O- und Ω-Notation:

Definition 2.4.1. O- und Ω-Notation
Sei $k \in \mathbb{N}$, $X, Y \subset \mathbb{N}^k$ und $f : X \to \mathbb{R}$, $g : Y \to \mathbb{R}$ Funktionen. Es ist $f = O(g)$, falls es positive reelle Zahlen B und C gibt, sodass für alle $(n_1, \ldots, n_k) \in \mathbb{N}^k$ mit $n_i > B,\ 1 \leq i \leq k$, folgendes gilt:

(i) $(n_1, \ldots, n_k) \in X \cap Y$, d.h. $f(n_1, \ldots, n_k)$ und $g(n_1, \ldots, n_k)$ sind definiert,

(ii) $f(n_1, \ldots, n_k) \leq Cg(n_1, \ldots, n_k)$.

Es ist also fast überall $f(n_1, \ldots, n_k) \leq Cg(n_1, \ldots, n_k)$ und man schreibt

$$g = \Omega(f)$$

[7], S.5.

Komplexitätsfunktionen lassen sich in verschiedene Klassen unterteilen. Die wichtigste Unterscheidung erfolgt in Probleme mit:

(i) **Polynomieller Komplexität:** Die benötigte Zeit oder der benötigte Raum wachsen in Abhängigkeit von n nur polynomiell. Die Komplexität beträgt also $O(g)$, wobei g eine Polynomfunktion ist.

(ii) **Exponentieller Komplexität:** Der zeitliche oder der räumliche Aufwand wächst exponentiell.

Im Allgemeinen werden Algorithmen mit polynomieller Komplexität als praktikabel oder effizient angesehen, während Algorithmen mit exponentieller Komplexität als ineffizient gelten. Natürlich gibt es auch Algorithmen mit polynomieller Komplexität, welche als unpraktikabel eingestuft würden: Je höher der Exponent, desto ineffizienter ist der Algorithmus. Tabelle 2.1 verdeutlicht dies. Sie bedient sich der Annahme eines Computers, der etwa eine Million Instruktionsschritte pro Sekunde durchführt.

Tabelle 2.1: Vergleich einiger Polynomial- und Exponentialfunktionen, [20], S.71

	n=10	**n=20**	**n=30**	**40**	**50**	**60**
n	0,00001 Sek.	0,00002 Sek.	0,00003 Sek.	0,00004 Sek.	0,00005 Sek.	0,00006 Sek.
n^2	0,0001 Sek.	0,0004 Sek.	0,0009 Sek.	0,0016 Sek.	0,0025 Sek.	0,0036 Sek.
n^3	0,001 Sek.	0,008 Sek.	0,027 Sek.	0,064 Sek.	0,125 Sek.	0,256 Sek.
n^5	0,1 Sek.	3,2 Sek.	24,3 Sek.	1,7 Min.	5,2 Min.	13,0 Min.
2^n	0,001 Sek.	1,0 Sek.	17,9 Min.	12,7 Tage	35,7 Jahre	366 Jhdte.
3^n	0,059 Sek.	58 Min	6,4 Jahre	3855 Jhdte.	$2 \cdot 10^8$ Jhdte.	$1{,}3 \cdot 10^{13}$ Jhdte.

In der Kryptographie wird nach Verschlüsselungsverfahren gesucht, bei welchen die regulären Teilnehmer mit polynomiellem Aufwand arbeiten können, während ein Angriff nur in exponentieller Zeit zu bewerkstelligen ist.

3 Symmetrische Verschlüsselungsverfahren

In diesem Kapitel werden symmetrische Verfahren vorgestellt, welche in der Vergangenheit von großer Bedeutung waren. Als ein Beispiel für Transpositionsverfahren wird die Skytala von Sparta beschrieben. Die Caesar- und die Vigenère-Verschlüsselung sind typische Vertreter monoalphabetischer bzw. polyalphabetischer affin linearer Verfahren.
Die einzelnen Verfahren werden zunächst beschrieben und anhand der in Abschnitt 2.1 erläuterten Merkmale charakterisiert. Anschließend wird jeweils betrachtet, unter welchen Umständen und mit welchen Mitteln ein Angreifer die Botschaften entschlüsseln kann.

3.1 Die Skytala von Sparta

Dieser Abschnitt basiert auf Beutelspacher, Kryptologie [3].
Die Skytala von Sparta wurde vor etwa 2500 Jahren entwickelt. Sie wurde von der Regierung Spartas genutzt, um verschlüsselte Botschaften an ihre Generäle zu versenden. Sender und Empfänger besaßen jeweils einen Zylinder mit gleichem Umfang (U), der in diesem Fall den Schlüssel darstellt. Wenn die Regierung einen Text verschlüsseln wollte, so wickelte der Schreiber einen schmalen Pergamentstreifen um den Zylinder und beschrieb diesen dann von links nach rechts (siehe Abbildung 3.1). Wurde das Pergament vom Zylinder genommen, so wurde die Nachricht dadurch unkenntlich. Erst die Generäle, die das Pergament um ihre eigene Skytala wickelten, konnten die Nachricht entziffern.

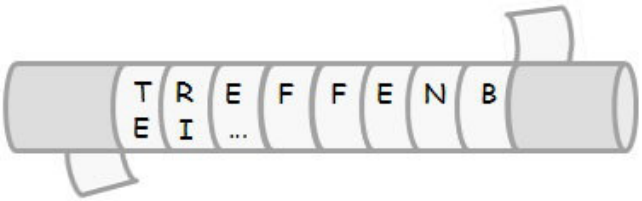


Abbildung 3.1: Skytala von Sparta, Quelle: Eigene Darstellung

Bei dieser Art der Verschlüsselung handelt es sich um ein Transpositionsverfahren. Sie kann auch ohne die Zylinder als Hilfsmittel durchgeführt werden. Man stelle sich dazu vor, der Umfang U würde durch die Anzahl der Buchstaben (u) repräseniert,

welche untereinander auf das Pergament passen, sobald es einmal umwickelt wurde. Verschlüsselt wird, indem der Klartext in eine Tabelle mit u Zeilen zeilenweise geschrieben, aber spaltenweise ausgelesen wird. Entschlüsselt wird der Geheimtext, indem er in eine Tabelle mit u Spalten wiederum zeilenweise eingeschrieben und spaltenweise ausgelesen wird. Der Schlüssel ist dabei die Anzahl u.

Verschlüsselungsverfahren 3.1.1. Die Skytala von Sparta
Sei $A = B = \{A, B, C, \ldots, Z\} \cup \{*\}$. Das Verfahren ist definiert durch:

(i) $M = C = A^l$, für ein $l \in \mathbb{N}$

(ii) $K = \{u \mid u \in \mathbb{N}\}$

(iii) $E_u : M \to C \; ; m \mapsto g \circ f_T(m), m = (m_1, m_2, \ldots, m_l, m_{l+1}, \ldots, m_{un})$ für $n \in \mathbb{N}$ mit $(u-1) \cdot n + 1 \leq l \leq u \cdot n$. Falls $l < u \cdot n$, setze: $m_{l+1} = \ldots = m_{un} = *$. Es ist

$$f : M \to \mathrm{Mat}^{u \times n} \text{ mit}$$

$$f(m) = \begin{pmatrix} m_1 & m_2 & \cdots & m_n \\ m_{n+1} & m_{n+2} & & \vdots \\ \vdots & & \ddots & \\ m_{(u-1)\cdot n+1} & \cdots & & m_{un} \end{pmatrix}$$

die Funktion, die die Nachricht m zeilenweise in eine Matrix $u \times n$ einschreibt,

$$f_T : \mathrm{Mat}^{u \times n} \to \mathrm{Mat}^{n \times u} \text{ mit}$$

$$f_T(m) = f(m)^T = \begin{pmatrix} m_1 & m_{n+1} & \cdots & m_{(u-1)\cdot n+1} \\ m_2 & m_{n+2} & & \vdots \\ \vdots & & \ddots & \\ m_n & \cdots & & m_{un} \end{pmatrix} =: X$$

die transponierte Matrix von $f(m)$ und

$$g : \mathrm{Mat}^{n \times u} \to C \text{ mit}$$

$$g(X) = (m_1, m_{n+1}, \ldots, m_{(u-1)\cdot n+1}, m_2, m_{n+2}, \ldots, m_n, \ldots m_{un}) = c$$

die Funktion, die X zeilenweise ausliest.

(iv) $D_u : C \to M \; ; c \mapsto g_D \circ f_{DT}(c)$, $c = (c_1, c_2, \ldots, c_l, \ldots, c_{un})$, wobei $f_D : C \to \mathrm{Mat}^{n \times u}$ die Funktion ist, die c zeilenweise in eine Matrix $n \times u$ einschreibt, f_{DT} deren Transponierte und

$g_D : \mathrm{Mat}^{u \times n} \to M$ die Funktion, die die Matrix $u \times n$ zeilenweise ausliest.

(v) Es gilt: $D_u(E_u(m)) = g_D \circ f_{DT} \circ g \circ f_T(m) = g_D(f_{DT}(g(X))) = g_D(f_{DT}(c)) = g_D(X^T) = m$.

Beispiel 3.1.2. Verschlüsselt werden soll der Klartext

$$TREFFENBEISONNENAUFGANG$$

mit dem Schlüssel $u = 3$. Es ist $l = 23$ und damit $n = 8$, da $(u-1) \cdot n + 1 = 17 \leq 23 \leq 24 = u \cdot n$. Es gilt dann:

$$m = (TREFFENBEISONNENAUFGANG*)$$

$$f(m) = \begin{pmatrix} T & R & E & F & F & E & N & B \\ E & I & S & O & N & N & E & N \\ A & U & F & G & A & N & G & * \end{pmatrix}$$

$$f_T(m) = \begin{pmatrix} T & E & A \\ R & I & U \\ E & S & F \\ F & O & G \\ F & N & A \\ E & N & N \\ N & E & G \\ B & N & * \end{pmatrix} = X$$

$$g(X) = c = (TEARIUESFFOGFNAENNNEGBN*)$$

Kryptoanalyse

Es werden nun die in Abschnitt 2.2 vorgestellten Angriffsszenarien betrachtet.

Known Ciphertext Attack

Angenommen Eve hat den Pergamentstreifen aus Beispiel 3.1.2, den Alice Bob zukommen lassen wollte, abgefangen. Anhand der vertikalen Schreibweise auf dem Papier vermutet sie, dass es sich um eine Verschlüsselung mit der Skytala handelt. Sie hat nun die Möglichkeit verschiedene Schlüssel zu testen und damit den richtigen zu finden. Wäre Eve's erste Wahl beispielsweise $u = 4$, so erhielte sie:

$$f_D(c) = \begin{pmatrix} T & E & A & R \\ I & U & E & S \\ F & F & O & G \\ F & N & A & E \\ N & N & N & E \\ G & B & N & * \end{pmatrix}$$

$$f_{DT}(c) = \begin{pmatrix} T & I & F & F & N & G \\ E & U & F & N & N & B \\ A & E & O & A & N & N \\ R & S & G & E & E & * \end{pmatrix}$$

und damit $m = (TIFFNGEUFNNBAEOANNRSGEE*)$. Sie müsste also weiter suchen, bis ein sinnvoller Text erscheint. Da Eve voraussichtlich als Schlüssel zunächst die Teiler der Nachrichtenlänge testet, kann Alice diesen Angriff erschweren, indem sie das letzte Geheimtextzeichen $*$ vor dem Versenden entfernt. Es ist für die Entschlüsselung durch Bob nicht relevant.

Known Plaintext Attack

In diesem Falle liegt Eve ein Stück des Klartextes vor. Es ist z. B. denkbar, dass sie weiß, dass Alice und Bob einen Treffpunkt vereinbaren wollen. Sie vermutet, dass der Klartext genau mit diesem Wort beginnt und sucht die entsprechenden Buchstaben: $c = \underline{T}EA\underline{R}IU\underline{E}SF\underline{F}OG\underline{F}NA\underline{E}NN\underline{N}EGBN$. Damit kann sie auf $u = 3$ schließen.

Chosen Plaintext (Ciphertext) Attack

Hier wird in zwei Fälle unterschieden: In Fall 1 verwenden Alice und Bob echte Zylinder zur Verschlüsselung. Hier wäre wieder der Umfang U und nicht u der Schlüssel. Hat Eve Zugang zur Skytala, kann sie zwar Nachrichten ver- oder entschlüsseln, hat aber keine Möglichkeit die Anzahl der Buchstaben, die Alice normalerweise in eine Spalte schreibt, zu ermitteln. Bob kann zwar die Nachricht entschlüsseln, bemerkt aber mit großer Wahrscheinlichkeit, dass die Nachricht gefälscht ist. In diesem Falle könnte man die Anzahl u als Signatur bezeichnen, also dem Zeichen von Alice, dass die Nachricht wirklich von ihr stammt.
In Fall 2 verwenden Alice und Bob ein Programm, dass nach dem Prinzip der Skytala verschlüsselt. Hat Eve Zugang zu diesem Programm inklusive des Schlüssels u, so kann sie Nachrichten verschlüsseln und u leicht auszählen. Bob hat keine Möglichkeit eine Fälschung zu bemerken.

Die beiden folgenden Abschnitte basieren weitesgehend auf den Büchern von Beutelspacher, [3] bzw. Ertel, [8].

3.2 Die Caesar-Verschlüsselung

Der römische Feldherr Julius Caesar (100 - 44 v. Chr.) verschlüsselte geheime Botschaften, indem er jeden Klartextbuchstaben durch den Buchstaben ersetzte, der im Alphabet 3 Stellen weiter rechts stand. Der Buchstabe A wurde also durch den Buchstaben D ersetzt, B durch E, C durch F usw. Man nennt dieses Verfahren auch *Verschiebechiffre*. Diese Art der Verschlüsselung funktioniert natürlich auch, wenn man die Buchstaben im Alphabet um beliebig viele Stellen verschiebt. Es gibt also genau 26 mögliche Verschiebungen. Leon Battista Alberti entwickelte 1470 die sogenannte Caesar-Scheibe, eine „Maschine“, mit welcher alle 26 Verschiebechiffren leicht genutzt werden können (siehe Abbildung 3.2). Durch Drehen der inneren

Scheibe können alle 26 möglichen Schlüssel eingestellt und die zum jeweiligen Klartextbuchstaben gehörenden Geheimtextbuchstaben direkt abgelesen werden.



Abbildung 3.2: Die Caesar-Scheibe, [1]

Um das Verfahren mathematischer darstellen zu können, werden die Buchstaben $A - Z$ im Alphabet mit den Zahlen $0 - 25$ identifiziert.

Verschlüsselungsverfahren 3.2.1. Die Caesar Verschlüsselung
Sei $A = B = \mathbb{Z}_{26}$. Das Verfahren ist definiert durch:

(i) $M = C = A^l$

(ii) $K = \mathbb{Z}_{26}$

(iii) $E_k : M \to C$; $m = (m_1, \ldots, m_l) \mapsto (m_1 + k \bmod 26, \ldots, m_l + k \bmod 26)$

(iv) $D_k : C \to M$; $c = (c_1, \ldots, c_l) \mapsto (c_1 - k \bmod 26, \ldots, c_l - k \bmod 26)$

(v) Es gilt: $D_k(E_k(m_i)) = ((m_i + k) \bmod 26) - k \bmod 26 = m_i$

Es handelt sich hierbei um eine affin lineare Chiffre mit $a = 1$ und $b = k$. Die Verschlüsselung ist monoalphabetisch.

Beispiel 3.2.2. Alice möchte den Klartext

$$m = TREFFENBEISONNENAUFGANG$$

diesmal mit der Caesar-Verschlüsselung chiffrieren. Sie wählt den Schlüssel $k = 5$ und erhält den Geheimtext:

$$c = YWJKKJSHJNXTSSJSFZKLFSL.$$

Kryptoanalyse

Auch für die Caesar-Verschlüsselung werden im Folgenden die einzelnen Angriffsszenarien beleuchtet.

Known Ciphertext Attack

Eve vermutet, dass der vorliegende Geheimtext mit der Caesar-Verschlüsselung chiffriert wurde. Sie hat die Möglichkeit, im Zuge einer *Brute Force Attack* alle 25 sinnvollen Schlüssel durchzuprobieren. Sie muss hierbei nicht immer den gesamten Geheimtext entschlüsseln, sondern kann sich z. B. auf die ersten 7 Buchstaben konzentrieren, um einen Schlüssel zu finden, bei welchem die Entschlüsselung einen sinnvollen Klartext ergibt.
Eine weitere Möglichkeit stellt die *statistische Analyse* dar: In der deutschen Sprache kommen die verschiedenen Buchstaben mit unterschiedlicher Häufigkeit vor. So ist z. B. der Buchstabe E mit Abstand der meist genutzte Buchstabe. Tabelle 3.1 zeigt die Häufigkeiten der Buchstaben in deutschen Texten.

Tabelle 3.1: Die Häufigkeiten der Buchstaben in deutschen Texten, nach [3], S.10.

Buchstabe	**Häufigkeit**	**Buchstabe**	**Häufigkeit**
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	2,35 %	Z	1,13 %

Bei der Verschlüsselung bleiben diese Häufigkeiten erhalten, übertragen sich allerdings auf den entsprechenden Geheimtextbuchstaben. Eve hat also die Möglichkeit den Buchstaben zu bestimmen, der im Geheimtext am häufigsten erscheint. Dieser entspricht mit großer Wahrscheinlichkeit dem Klartextbuchstaben E. Im Fall aus Beispiel 3.2.2 würde Eve den Buchstaben S mit E identifizieren und somit fälschlicherweise auf den Schlüssel 14 schließen. Erst im zweiten Anlauf, wenn sie den zweithäufigsten Buchstaben J mit dem E identifiziert, würde sie den richtigen Schlüssel $k = 5$ erhalten. Trotz eines Fehlversuches wäre sie schneller am Ziel, als bei einer *Brute Force Attack*. Allgemein ist zu erkennen, dass solche statistischen Analysen zuverlässiger werden, je länger der Geheimtext ist.

Known Plaintext Attack

Hat Eve eine Vermutung über den Beginn oder eine andere Stelle des Klartextes, so testet sie ihre Hypothese, indem sie den vermuteten Schlüssel ermittelt und mit ihm einen Stück des Textes entschlüsselt.

Chosen Plaintext (Ciphertext) Attack

Hat Eve Zugang zu dem Programm mit gespeichertem Schlüssel, so kann sie einen Klartext verschlüsseln lassen, z. B. den Text $m = a$ und den Schlüssel ablesen. Falls Bob sonst keine weiteren Vereinbarungen mit Alice getroffen hat, wie z. B. die Nutzung einer bestimmten Begrüßungsfloskel, so kann er eine Fälschung von Eve nicht erkennen.

Monoalphabetische Verschlüsselungen sind also durch statistische Analysen recht einfach zu brechen. Um Verschlüsselungssysteme sicherer zu gestalten, müssen die Häufigkeiten der Buchstaben angeglichen werden. Dafür gibt es zwei Möglichkeiten:

1. Die **homophone Chiffrierung**: Ziel dieser Verschlüsselung ist es, dass jeder Geheimtextbuchstabe etwa gleich häufig vorkommt. Dazu werden jedem Klartextbuchstaben, entsprechend seiner Häufigkeit in deutschen Texten, mehrere Geheimtextbuchstaben zugeordnet. Als Geheimtextalphabet eignen sich z. B. die Zahlen $00 - 99$. Tabelle 3.2 zeigt eine mögliche, homophone Chiffrierung.

Tabelle 3.2: Eine homophone Chiffrierung, nach [3], S.28

Buchstabe	Zugeordnete Zeichen	Buchstabe	Zugeordnete Zeichen
A	10 21 52 59 71	N	30 35 43 62 63 67 68 72 77 79
B	20 34	O	02 05 82
C	28 06 80	P	31
D	04 19 70 81 87	Q	25
E	09 18 33 40 42 53 54 55 60 66 75 85 86 92 93 99	R	17 36 51 69 74 78 83
F	00 41	S	15 26 45 56 61 73 96
G	08 12 97	T	13 32 90 91 95 98
H	07 24 47 89	U	29 01 58
I	14 39 46 50 65 76 88 94	V	37
J	57	W	22
K	23	X	44
L	16 03 84	Y	48
M	27 11 49	Z	64

   Dem E, welches eine Häufigkeit von über 17% aufweist, werden 17 Geheimtextbuchstaben zugeordnet. Dem F dagegen werden, entsprechend seiner Häu-

figkeit von knapp 2%, zwei Geheimtextzeichen zugeordnet. Für eine eindeutige Entschlüsselung ist wichtig, dass die Mengen von Geheimtextzeichen disjunkt sind. Allerdings ist auch diese Methode nicht sicher vor Angreifern. Statistische Analysen sind möglich. Hilfreich sind dabei Bigramme, Buchstabenpaare wie z. B. *en* oder *ch*, welche in der deutschen Sprache häufig gemeinsam auftreten.

2. Die **Vigenère-Verschlüsselung**, die im folgenden Abschnitt ausführlich beschrieben wird.

3.3 Die Vigenère-Verschlüsselung

Der französische Diplomat Blaise de Vigenère veröffentlichte die Vigenère-Chiffre im Jahre 1586. Das Prinzip der Verschlüsselung beruht auf dem periodischen Wechsel verschiedener monoalphabetischer Chiffren. Um eine Nachricht „per Hand“ zu verschlüsseln, wird das sogenannte Vigenère-Quadrat benötigt (siehe Abbildung 3.3). In ihm sind alle 26 Verschiebechiffren untereinander aufgelistet, das heißt es gibt für jeden Buchstaben des Alphabets jeweils eine Zeile, die mit diesem Buchstaben beginnt.

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 3.3: Das Vigenère-Quadrat, [3], S.30

Des Weiteren wird eine beliebige Buchstabenfolge, das Schlüsselwort, benötigt.

Dieses wird über den Klartext geschrieben - solange, bis das Ende des Klartextes erreicht ist. Jeder Buchstabe wird nun verschlüsselt, indem diejenige Zeile des Vigenère-Quadrats genutzt wird, welche mit dem darüberstehenden Schlüsselwortbuchstaben beginnt.

Beispiel 3.3.1. Wieder soll der Klartext aus Beispiel 3.1.2 verschlüsselt werden. Das Schlüsselwort lautet *GEHEIM*.

Schlüsselwort:	G	E	H	E	I	M	G	E	H	E	I	M	G	E	H	E	I	M	G	E	H	E	I	M	G	E
Klartext:		T	R	E	F	F	P	U	N	K	T	B	E	I	S	O	N	N	E	N	A	U	F	G	A	N	G
Geheimtext:		Z	V	L	J	N	B	A	R	R	X	J	Q	O	W	V	R	V	Q	T	E	B	J	O	M	T	K

Der Vorteil der polyalphabetischen Verschlüsselungsmethode wird hierbei deutlich: Gleiche Klartextbuchstaben werden meistens in unterschiedliche Geheimtextbuchstaben verschlüsselt (F an Position 4 und 5). Es kann aber auch vorkommen, dass unterschiedliche Klartextbuchstaben zu gleichen Geheimtextbuchstaben führen (R an Position 8 und 9).

Verschlüsselungsverfahren 3.3.2. Die Vigenère-Verschlüsselung
Sei $A = B = \mathbb{Z}_{26}$. Das Verfahren ist definiert durch:

(i) $M = C = A^l$

(ii) $K \subseteq A^*$ als Menge der Schlüsselwörter beliebiger Länge

(iii) $E_k : M \to C$, $k = (k_0, \ldots, k_{n-1}) \in K$; für $m = (m_1, \ldots, m_l) \in M$ gilt:
$m_i \mapsto (m_i + k_{i \bmod n}) \bmod 26$, $i \in \{1, \ldots, l\}$

(iv) $D_k : C \to M$; für $c = (c_1, \ldots, c_l) \in C$ gilt:
$c_i \mapsto (c_i - k_{i \bmod n}) \bmod 26$, $i \in \{1, \ldots, l\}$

(v) $D_k(E_k(m_i)) = ((m_i + k_{i \bmod n}) \bmod 26) - k_{i \bmod n} \bmod 26 = m_i$

Das Verfahren kann als eine affin lineare Chiffre mit

$$a = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \in \mathrm{Mat}^{l \times l}$$

und

$$b = \begin{pmatrix} k_0 \\ \vdots \\ k_{n-1} \\ k_0 \\ \vdots \end{pmatrix} \in A^l$$

aufgefasst werden.

Kryptoanalyse

Obwohl die Vigenère-Verschlüsselung schon wesentlich sicherer als die monoalphabetische Caesar-Verschlüsselung erscheint, hat Eve jedoch gute Chancen, auch diesen Code zu knacken.

Known Ciphertext Attack

Angenommen Eve fängt den folgenden Geheimtext ab[1]:

```
WUBE FIQL ZURM VOFE HMYM WTIX CGTM PIFK RZUP MVOI RQMM WOZM
PULM BNYV QQQM VMVJ LEYM HFEF NZPS DLPP SDLP EVQM WCXY MDAV
QEEF IQCA YTQO WCXY MWMS EMEF CFWY EYQE TRLI QYCG MTWC WFBS
MYFP LRXT QYEE XMRU LUKS GWFP TLRQ AERL UVPM VYQY CXTW FQLM
TELS FJPQ EHMO ZCIW CI WF PZSL MAEZ IQVL QMZV PPXA WCS M ZMOR
VGVV QSZE TRLQ ZPBJ AZVQ I YXE WWOI CCGD WHQM MVOW S GNT J PFP
PAYB IYBJ UTWR LQKL KLLL MDPY VACD CFQN ZPIF PPKS DVPT I DGX
MQQV EBMQ ALKE ZMGC VKUZ KI ZB ZLI U AMMV Z
```

Sie vermutet, dass der Text mit dem Vigenère-Verfahren verschlüsselt wurde, da eine einfache statistische Analyse nicht zum Erfolg führte. Um den Text zu entschlüsseln, geht sie folgendermaßen vor:

1. Durchführung des *Kasiski-Tests*: Mithilfe dieses Tests erhält Eve mögliche Schlüssellängen (bis auf Vielfache).

2. Durchführung des *Friedmann-Tests*: Eve erhält die ungefähre Größenordnung des Schlüssels und kann mit den Ergebnissen aus 1. die Schlüssellänge n bestimmen.

3. Der Geheimtext lässt sich in n Teiltexte aufteilen. Jeder der Teiltexte entstand durch Verschlüsselung mit einem Schlüsselzeichen, also monoalphabetisch. Eve kann mittels Häufigkeitsanalyse die jeweiligen Schlüsselzeichen bestimmen und erhält damit das Schlüsselwort.

Der Kasiski- (Abschnitt 3.3.1) und der Friedmann-Test (Abschnitt 3.3.2) sind wichtige Methoden und werden daher später ausführlich dargestellt. Die Ausführungen beruhen auf den Büchern „Kryptologie“ von Beutelpacher [3] und „Angewandte Kryptographie“ von Ertel [8].

Known Plaintext Attack

Natürlich hat Eve auch hier wieder einen Vorteil, wenn sie Bruchstücke des Klartextes kennt. Zunächst berechnet sie aus den einzelnen Paaren von Buchstaben Teile des Schlüssels. Sie erkennt die Schlüssellänge aber erst bei ausreichend vielen zusammenhängenden Paaren, sodass die erhaltene Schlüsselfolge erkennbar periodisch wird. Durch Abzählen der Positionen vor dem bekannten Stück Text, erhält sie dann den richtigen Beginn des Schlüssels.

[1] Das Beispiel wurde dem Buch Geheime Botschaften von Simon Singh ([21], S.65 ff) entnommen.

Chosen Plaintext (Ciphertext) Attack

Hat Eve Zugang zum Algorithmus ohne das Schlüsselwort zu kennen, so hat sie leichtes Spiel: Sie kann einen beliebigen Text (am einfachsten bestünde dieser nur aus dem Buchstaben a) ver- oder entschlüsseln lassen und kann mit dem Ergebnis das Schlüsselwort berechnen.

3.3.1 Der Kasiski-Test

Der Kasiski-Test wurde von dem preußischen Major Friedrich Kasiski im Jahre 1863 veröffentlicht. Entwickelt wurde er aber bereits von Charles Babbage im Jahre 1854. Der Test beruht auf folgender Tatsache: Gleiche Klartextpassagen, deren Abstand ein Vielfaches der Schlüssellänge n ist, ergeben gleiche Geheimtextpassagen. Aufgabe des Angreifers ist es also zunächst, den Geheimtext nach Wiederholungen von mindestens drei Zeichen abzusuchen. Die Abstände dieser Passagen werden notiert und in ihrer Primfaktorzerlegung dargestellt. Der größte gemeinsame Teiler aller Abstände (oder ein Vielfaches davon) wird als Schlüssellänge vermutet. Da Wiederholungen im Geheimtext auch zufälligerweise auftreten können, müssen Ausreißer aus der Betrachtung genommen werden, da sonst der größte gemeinsame Teiler schnell 1 wird.

Beispiel 3.3.3. Eve findet drei Passagen, die wiederholt auftreten:

```
WUBE FI QL ZURM VOFE HMYM WTIX CGTM PI FK RZUP MVOI RQMM WOZM
PULM BNYV QQQM VMVJ LEYM HFEF NZPS DLPP SDLP EVQM WCXY MDAV
QEEF IQCA YTQO WCXY MWMS EMEF CFWY EYQE TRLI QYCG MTWC WFBS
MYFP LRXT QYEE XMRU LUKS GWFP TLRQ AERL UVPM VYQY CXTW FQLM
TELS FJPQ EHMO ZCIW CI WF PZSL MAEZ IQVL QMZV PPXA WCS M ZMOR
VGVV QSZE TRLQ ZPBJ AZVQ I YXE WWOI CCGD WHQM MVOW S GNT J PFP
PAYB IYBJ UTWR LQKL KLLL MDPY VACD CFQN ZPIF PPKS DVPT I DGX
MQQV EBMQ ALKE ZMGC VKUZ KI ZB ZLIU AMMV Z
```

Für die Abstände A gilt:

$$\begin{aligned} A_{PSDLP} &= 5 \\ A_{WCXYM} = 20 &= 2^2 \cdot 5 \\ A_{ETRL} = 120 &= 2^3 \cdot 3 \cdot 5 \end{aligned}$$

Der größte gemeinsame Teiler beträgt 5. Eve vermutet also eine Schlüssellänge von

$$n = 5x,\ x \in \mathbb{N}.$$

3.3.2 Der Friedmann-Test

William Friedmann entwickelte 1925 einen Test zur näherungsweisen Bestimmung der Schlüssellänge n. Die Idee dahinter: Innerhalb der n Teiltexte, die jeweils monoalphabetisch kodiert sind, gibt es mehr Wiederholungen von Buchstaben, als zwischen den Teiltexten.

Definition 3.3.4. Der *Koinzidenzindex I* gibt die Wahrscheinlichkeit an, dass zwei zufällig aus einem Text gegriffene Buchstaben gleich sind. Es gilt:

$$I = \sum_{i=1}^{26} \frac{m_i(m_i - 1)}{m(m-1)}$$

Herleitung:
Sei m_1 die Häufigkeit des Buchstaben a, m_2 die Häufigkeit des Buchstaben b, usw. Dann gilt für die Länge m des Klartextes:

$$m = \sum_{i=1}^{26} m_i$$

Weiterhin gibt es genau

$$\frac{m(m-1)}{2}$$

Paare von Buchstaben im Klartext. Für die Anzahl der Paare (a,a) gilt:

$$\frac{m_1(m_1 - 1)}{2}$$

und damit für die Summe aller Paare aus gleichen Buchstaben:

$$\sum_{i=1}^{26} \frac{m_i(m_i - 1)}{2}$$

Der Koinzidenzindex ergibt sich nun aus dem Verhältnis aller Paare mit gleichen Buchstaben zu allen möglichen Paaren.

Bemerkung 3.3.5.

(i) Für lange deutsche Texte kann der Koinzidenzindex mithilfe der Wahrscheinlichkeiten aus Tabelle 3.1 berechnet werden. Es gilt: $I_d \approx 0,0762$. Dieser Index gilt damit auch für die n Teiltexte, die jeweils monoalphabetisch verschlüsselt wurden. Für englische Texte gilt $I_e \approx 0,0661$.

(ii) Für lange zufällige Texte, in denen die Wahrscheinlichkeiten der Buchstaben gleichverteilt und damit die Häufigkeiten m_i für alle Buchstaben gleich sind, gilt: $I_r \approx 0,0385$. Dieser Index gilt demnach für Buchstaben aus unterschiedlichen Teiltexten.

Bei n Teiltexten enthält jeder Teiltext etwa m/n Buchstaben. Für die Anzahl der Paare aus gleichen Buchstaben innerhalb der Teiltexte gilt demnach:

$$\frac{1}{2} \cdot \frac{m}{n} \cdot (\frac{m}{n} - 1) \cdot k = \frac{m(m-n)}{2n}$$

Für die Anzahl der Paare aus gleichen Buchstaben von verschiedenen Teiltexten gilt:

$$m \cdot (m - \frac{m}{n}) \cdot \frac{1}{2} = \frac{m^2(n-1)}{2n}$$

Es ergibt sich für den gesamten Text:

$$\frac{m(m-n)}{2n} \cdot I_d + \frac{m^2(n-1)}{2n} \cdot I_r$$

Division durch die Zahl der Paare insgesamt liefert die Wahrscheinlichkeit für Paare aus gleichen Buchstaben, die ungefähr gleich dem Koinzidenzindex sein muss:

$$I \approx \frac{(m-n)}{(m-1)n} \cdot I_d + \frac{m(n-1)}{(m-1)n} \cdot I_r$$

Nach n aufgelöst ergibt dies eine Formel zur näherungsweisen Bestimmung der Schlüssellänge:

$$\boxed{n \approx \frac{(I_d - I_r)m}{(m-1)I - I_r m + I_d} = \frac{0,0377m}{(m-1)I - 0,0385m + 0,0762}}$$

Beispiel 3.3.6. Aus den Häufigkeiten der einzelnen Buchstaben im Text ergibt sich ein Koinzidenzindex von $I = 0,04657$. Eve weiß, dass der Text höchstwahrscheinlich in englischer Sprache verfasst wurde. Mit einer Textlänge von $m = 369$ ergibt sich eine Schlüssellänge von $n \approx 4,64$. Interpretiert man dieses Ergebnis auf der Grundlage des Kasiski-Tests, so bestätigt sich die Schlüssellänge 5. Die statistische Analyse der Teiltexte ergibt das Schlüsselwort $EMILY$.
Bei der Entschlüsselung entsteht in der Tat ein sinnvoller englischer Text, ein Gedicht von Alfred Tennyson, welches in Anhang B zu lesen ist.

4 Public-Key-Verfahren

Die bisher vorgestellten symmetrischen Verfahren haben ein zentrales Problem gemein: Das Schlüsselaustauschproblem. Bevor sich Alice und Bob verschlüsselte Nachrichten zukommen lassen können, müssen sie den Schlüssel zuvor über einen sicheren Kanal austauschen. Bei zwei Teilnehmern ist diese Aufgabe noch übersichtlich und meist gut zu bewerkstelligen. Doch wie wäre es bei n Teilnehmern? Wenn je zwei dieser Teilnehmer einen Schlüssel austauschen, so müssen schon $n(n-1)/2$ Schlüssel übertragen werden. Bei z. B. 1000 Teilnehmern wären das 499500 Schlüssel.
Dieses Problem kann durch die Nutzung von Public-Key-Verfahren umgangen werden. Die Idee eines solchen asymmetrischen Verfahrens wurde schon in Abschnitt 2.1 vorgestellt. Jeder der n Teilnehmer besitzt einen öffentlichen Schlüssel. Diese können in einem Verzeichnis, wie etwa in einem Telefonbuch, festgehalten und öffentlich gemacht werden ([7], Kapitel 7). Das bekannteste solcher Verfahren, der **RSA-Algorithmus**, wird in Abschnitt 4.1 vorgestellt.
Die Verschlüsselung von Nachrichten mithilfe von asymmetrischen Verfahren hat allerdings einen entscheidenden Nachteil: Der zeitliche Aufwand ist wesentlich höher als bei symmetrischen Verfahren ([3], S.115). In sogenannten *hybriden Verfahren* werden symmetrische Verfahren zur Verschlüsselung der Nachrichten verwendet. Asymmetrische Verfahren dienen lediglich dem Schlüsselaustausch. Die geringe Geschwindigkeit spielt hierbei keine entscheidende Rolle, da die Schlüssel wesentlich kleiner sind als die zu verschlüsselnde Nachricht. Ein sehr bekanntes **Schlüsselaustauschverfahren von Diffie & Hellman** wird in Abschnitt 4.2 beschrieben.

4.1 Das RSA-Verfahren

Dieses Verfahren wurde im Jahre 1978 vorgestellt. Benannt ist es nach seinen Entwicklern Ron **R**ivest, Adi **S**hamir und Leonard **A**dleman. Zunächst wird der Algorithmus beschrieben und seine Korrektheit gezeigt. Anschließend soll auch hier ein Blick auf die Sicherheit des Verfahrens geworfen werden.

4.1.1 Der Algorithmus

Die zentrale Idee des Public-Key-Verfahrens ist die Bereitstellung von öffentlichen Schlüsseln. Die Schlüsselerzeugung für den RSA-Algorithmus funktioniert dabei wie folgt [8]:

Definition 4.1.1. Schlüsselerzeugung
Folgende Schritte sind durchzuführen:

1. Zufällige Wahl von $p, q \in \mathbb{P}, p \neq q$ mit einer Länge von 384 -512 Bit (entspricht etwa 116-154 Dezimalstellen).
2. Berechnung von $n = p \cdot q$.
3. Wahl von $e \in \mathbb{N}$, ungerade, $1 < e < \varphi(n)$, sodass für $\varphi(n) = (p-1)(q-1)$ gilt: $\text{ggt}(e, \varphi(n)) = 1$.
4. Berechnung von d mit $ed \equiv 1 \bmod \varphi(n)$[1].
5. Bekanntgabe des öffentlichen Schlüssels (e, n).
6. Geheimhaltung des privaten Schlüssels d.

Bei der Wahl der Primzahlen p und q sowie von e sind einige Aspekte zu berücksichtigen. Diese werden in Abschnitt 4.1.2 näher beschrieben.

Verschlüsselungsverfahren 4.1.2. Der RSA-Algorithmus
Sei $A = B = \mathbb{Z}_n$. Das Verfahren ist definiert durch:

(i) $M = C \subseteq A^*$

(ii) $K = \{((e,n), d) : (e,n) \in \mathbb{N} \times \mathbb{N}, \text{ggt}(e, \varphi(n)) = 1, d \in \mathbb{N} : ed \equiv 1 \bmod \varphi(n)\}$.

(iii) Für $m \in M$, $m < n$ gilt:

$$E_{(e,n)} : M \to C;$$
$$m \mapsto m^e \bmod n.^2$$

Für $m \geq n$ teile m in Blöcke m_i mit $m_i < n$ und

$$m = (m_1, m_2, \ldots) \mapsto (m_1^e \bmod n,\, m_2^e \bmod n, \ldots).$$

(iv) Für $c \in C$, $c < n$ gilt:

$$D_d : C \to M;$$
$$c \mapsto c^d \bmod n.$$

Für $c \geq n$ teile c in Blöcke c_i mit $c_i < n$ und

$$c = (c_1, c_2, \ldots) \mapsto (c_1^d \bmod n,\, c_2^d \bmod n, \ldots).$$

(v) Es gilt: $D_d(E_{(e,n)}(m)) = m$ für alle $m \in M$ (siehe Satz 4.1.4).

Das folgende Beispiel soll die Vorgehensweise bei der Verschlüsselung verdeutlichen. Die Zahlen sind sehr klein gehalten, das Verfahren wäre bei ihrer Verwendung sehr unsicher.

[1] Die Berechnung erfolgt mit dem erweiterten euklidischen Algorithmus, siehe Anhang A2.

[2] Die modulare Exponentiation durch schrittweise Multiplikation von m mit sich selbst ist sehr zeitaufwändig. Mit dem *„Square-And-Multiply"*-Algorithmus kann die Effizienz wesentlich erhöht werden. Der Algorithmus ist ist Anhang A2 beschrieben.

Beispiel 4.1.3. Seien $p = 71$ und $q = 103$ Primzahlen. Dann ist

$$n = pq = 7313$$

und

$$\varphi(n) = (p-1)(q-1) = 70 \cdot 102 = 7140.$$

Wähle $e = 43$ mit $\text{ggt}(43, 7140) = 1$. Es folgt

$$d = 43^{-1} \bmod 7140 = 3487,$$

denn

$$3487 \cdot 43 = 149941 = 21 \cdot 7140 + 1 \equiv 1 \bmod 7140.$$

Alice möchte die Nachricht

$$TREFFPUNKTBEISONNENAUFGANG$$

verschlüsseln. Die Buchstaben werden in natürliche Zahlen in 26-adischer Darstellung[3] kodiert.
Die Blocklänge beträgt $l = \lfloor \log_{26} 7313 \rfloor = 2$. Die Nachricht wird also in Blöcke der Länge zwei unterteilt und die einzelnen Buchstaben mit den Zahlen $0 - 25$ identifiziert. Für den Beginn der Nachricht gilt:

T	R	E	F	F	...
19	17	4	5	5	...

$$19 \cdot 26^1 + 17 \cdot 26^0 = 494 + 17 = 511$$
$$4 \cdot 26^1 + 5 \cdot 26^0 = 104 + 5 = 109$$

Es ergibt sich die Nachricht:

$$m = 511 \;\; 109 \;\; \ldots \in \mathbb{Z}_{7313}^*$$

Es folgt die Verschlüsselung mit dem öffentlichen Schlüssel $(43, 7313)$:

$$511^{43} \bmod 7313 = 6294$$
$$109^{43} \bmod 7313 = 4182.$$

Damit lautet der Geheimtext

$$c = 6294 \;\; 4182 \;\; \ldots \in \mathbb{Z}_{7313}^*$$

In der Tat erhält Bob durch Anwendung des geheimen Schlüssels den Klartext m, denn:

$$6294^{3487} \bmod 7313 = 511$$
$$4182^{3487} \bmod 7313 = 109.$$

[3] Eine Definition der g-adischen Darstellung befindet sich im Anhang A2.

Die Entschlüsselung bzw. die Korrektheit des Algorithmus beruht auf folgendem Satz ([7], S.118):

Satz 4.1.4. Korrektheit des Algorithmus
Sei (n, e) der öffentliche Schlüssel und d der geheime Schlüssel. Dann gilt für alle $m \in M$ mit $0 \leq m < n$:

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

Beweis
Nach Definition 4.1.1 gilt:

$$ed \equiv 1 \bmod \varphi(n).$$

Es existiert also ein $k \in \mathbb{N}$ sodass gilt:

$$ed = 1 + k(p-1)(q-1).$$

Daraus folgt:

$$(m^e)^d = m^{ed} = m^{1+k(p-1)(q-1)} = m(m^{k(p-1)(q-1)}) = m(m^{p-1})^{k(q-1)}$$

und damit gilt:

$$(m^e)^d \equiv m \bmod p,$$

denn falls p nicht m teilt, so ist $\text{ggt}(p, m) = 1$ und nach dem kleinen Satz von Fermat[4] $m^{p-1} \equiv 1 \bmod p$. Falls p ein Teiler von m ist, so ist die Äquivalenz trivial. Analog gilt auch:

$$(m^e)^d \equiv m \bmod q.$$

Da p und q verschiedene Primzahlen sind, gilt nach dem Chinesischen Restsatz[5]:

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

□

4.1.2 Sicherheit

Die Ausführungen in diesem Abschnitt beruhen weitestgehend auf dem Buch von Rothe, [20], Kapitel 7.
Das RSA-Kryptosystem verwendet große Primzahlen für die Berechnung des Moduls n. Um Primzahlen zu erhalten, werden meist Zufallszahlen erzeugt und anschließend einem Primzahltest unterworfen. Die ausführliche Behandlung solcher Tests ist nicht Bestandteil dieser Arbeit, kann aber in der Literatur zu diesem Kapitel nachgeschlagen werden. Es sei allerdings darauf hingewiesen, dass das Primzahlproblem in polynomieller Zeit, also relativ schnell, gelöst werden kann.

[4] Nachzulesen in Anhang A2
[5] Nachzulesen in Anhang A2

Die Sicherheit des RSA-Kryptosystems beruht auf einem anderen mathematischen Problem: Dem Faktorisierungsproblem. Man nimmt an, dass Zahlen mit einer Länge von 1024 Bits nicht, oder nur in sub-exponentieller Zeit[6], in ihre Primfaktoren zerlegt werden können. Für die Verwendung des RSA-Algorithmus bedeutet dies, dass, bei einer Wahl von p und q mit jeweils etwa 512 Bits, der Algorithmus nicht gebrochen werden kann. Diese Annahme ist allerdings nicht bewiesen. Zum einen ist bisher nicht auszuschließen, dass ein Angreifer ohne Faktorisierung von n Informationen über den Klartext oder den Schlüssel erhalten kann. Zum anderen muss auch damit gerechnet werden, dass das Faktorisierungsproblem irgendwann in polynomieller Laufzeit zu lösen ist.
In diesem Abschnitt werden zunächst mögliche **Faktorisierungsangriffe** vorgestellt. Je nach Wahl der einzelnen Parameter ergeben sich **weitere Angriffsmöglichkeiten**, die im Anschluss beschrieben werden. Die Liste der Angriffsmöglichkeiten auf den RSA-Algorithmus ist damit längst nicht vollständig. Zusammenfassend werden **Empfehlungen** zur Wahl der einzelnen Parameter gesammelt.

4.1.2.1 Faktorisierungsangriffe

Um eine Nachricht entschlüsseln zu können, benötigt Eve den geheimen Schlüssel d. Die beiden Probleme, nämlich

- die Bestimmung von d aus (e, n)
- die Zahl n in p und q zu zerlegen

sind algorithmisch äquivalent.
Karpfinger [11], S.122 gibt dazu jeweils einen polynomialen Algorithmus an, der das eine in das andere Problem überführt:
Falls es Eve gelingt aus dem Modul n die Primzahlen p und q zu bestimmen, so kann sie $\varphi(n) = (p-1)(q-1)$ berechnen und erhält mit Anwendung des erweiterten euklidischen Algorithmus den geheimen Schlüssel d als das Inverse zu e modulo $\varphi(n)$. Der zweite Algorithmus ist wesentlich komplizierter und soll daher in dieser Arbeit nicht aufgeführt werden.
Aus dieser Äquivalenz folgt, dass, neben der Faktorisierung, auch das Brechen des RSA-Algorithmus als schwieriges Problem angesehen wird.
Im Folgenden werden verschiedene Möglichkeiten zur Faktorisierung aufgezeigt. Eine geeignete Wahl der Parameter kann diese Angriffe erfolglos werden lassen.

Brute Force Angriff

Eve hat die Möglichkeit eine der Primzahlen durch *Probedivision* zu erhalten: Dabei bestimmt sie von allen Primzahlen, die kleiner als eine gewisse Schranke B sind, die größte Potenz von p, die n teilt. Eine typische Schranke liegt bei $B = 1000000$.

[6] Der zugehörige Algorithmus läuft zwar nicht in polynomieller, jedoch schneller als in exponentieller Zeit.

Für $l = \lfloor \log n \rfloor + 1$, als Länge der Binärdarstellung von n, liegt die Laufzeit des Algorithmus bei $O(2^{l/2})$ ([20], S.357).
Diesem Angriff kann durch hinreichend großem n entgegengewirkt werden. Auch ist zu empfehlen die Primzahlen p und q etwa gleichgroß zu wählen.

Pollards (p-1) Methode

Diese Methode, die 1974 von John Pollard entwickelt wurde, kann Zahlen mit einer ganz bestimmten Eigenschaft besonders gut faktorisieren. Es geht dabei um Module n mit Primfaktor p, sodass $p-1$ nur kleine Primfaktoren hat. Solche Zahlen sollten beim Gebrauch des RSA-Verfahrens vermieden werden, [7], Abschnitt 8.2.
Es ist zunächst ein Vielfaches k der Zahl $p-1$ gesucht. Als Kandidat für ein Vielfaches dient

$$k = \prod_{q \in \mathbb{P},\ q^e \leq B} q^e$$

für eine Schranke B.
Wenn alle Primzahlpotenzen, die $p-1$ teilen, kleiner gleich dieser Schranke sind, dann ist k ein Vielfaches von $p-1$. Hier wird nun deutlich, warum diese Methode besonders geeignet ist, wenn $p-1$ kleine Primfaktoren besitzt.
Für $k = x \cdot (p-1)$ für ein $x \in \mathbb{N}$ gilt nach dem kleinen Satz von Fermat:

$$a^k = (a^{p-1})^x \equiv 1 \bmod p$$

für ein a mit $\mathrm{ggt}(a, n) = 1$. Daraus folgt:

$$p | a^k - 1.$$

Falls nun $n \nmid a^{k-1}$, dann folgt $\mathrm{ggt}(a^k - 1, n) | n$ und damit ist ein Primfaktor von n gefunden. Falls kein Faktor gefunden wird, so muss die Schranke B erhöht werden.

Die Laufzeit des Algorithmus beträgt $O(B \log(B) l^2 + l^3)$, wobei l dabei wieder die Länge von n ist ([20], S.384). Der Algorithmus läuft also in Polynomialzeit, falls B polynomiell ist. Um diesen Angriff auszuschließen, empfiehlt es sich, die Primzahlen p und q so zu wählen, dass $p-1$ einen großen Primteiler r und $q-1$ einen großen Primteiler s besitzt.

Das folgende Beispiel soll anhand von kleinen Zahlen das Vorgehen verdeutlichen.

Beispiel 4.1.5. Die Zahl $n = 1241143$ soll faktorisiert werden. Mit $B = 13$ ist

$$k = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$$

und

$$\mathrm{ggt}(2^k - 1, n) = 547.$$

Es ist tatsächlich $547 \cdot 2269 = 1241143$ und beide Faktoren sind Primzahlen.

Das quadratische Sieb

Das quadratische Sieb ist eine sehr effiziente Faktorisierungsmethode, die nicht von bestimmten Eigenschaften von p und q abhängt. Sie wird beschrieben nach Buchmann [7], Abschnitt 8.3.

Idee

Das Ziel ist es, einen echten Teiler des Moduls n zu finden. Dazu werden ganze Zahlen x und y bestimmt, mit

$$x^2 \equiv y^2 \bmod n$$

und

$$x \not\equiv \pm y \bmod n$$

Es gilt dann:

$$n | x^2 - y^2 = (x-y)(x+y)$$
$$\text{aber}$$
$$n \not| (x-y) \text{ und } n \not| (x+y)$$

Damit ist $g = \text{ggt}(x-y, n)$ ein echter Teiler von n.

Bestimmung von x und y

Es sei

$$m = \lfloor \sqrt{n} \rfloor$$

und

$$f(X) = (X+m)^2 - n$$

Für geeignete s, sodass $f(s)$ nur kleine Primfaktoren hat, gilt jeweils:

$$(s+m)^2 \equiv f(s) \bmod n$$

Um eine Gleichung der Form $x^2 \equiv y^2 \bmod n$ zu erhalten, werden nun zwei Kongruenzen ausgewählt und multipliziert. Die linke Seite ergibt dabei immer ein Quadrat. Auf der rechten Seite erhält man ein Quadrat, wenn die Exponenten der Primfaktoren und der -1 gerade sind.

Beispiel 4.1.6.

Sei $n = 7429$. Damit ist $m = 86$ und $f(X) = (X+86)^2 - 7429$. Es werden nun geeignete Zahlen s gesucht.

Bestimmung geeigneter Zahlen s

Definition 4.1.7.

- $F(B) = \{p \in \mathbb{P} : p \leq B\} \cup \{-1\}$ heißt *Faktorbasis*.
- Die Funktionswerte $f(s)$ heißen *B-glatt*, falls alle Primfaktoren von $f(s)$ in $F(B)$ enthalten sind.

Gesucht sind Zahlen s für die $f(s)$ B-glatt ist. Das hier vorgestellte Verfahren ist das eigentliche „Sieb“, nachdem diese Faktorisierungsmethode benannt ist. Folgende Schritte müssen durchlaufen werden:

- Lege Siebintervall $S = \{-C, -C+1, \ldots, 0, 1, \ldots, C\}$ mit $C \in \mathbb{Z}$ fest.
- Berechne $f(s)$ für alle $s \in S$.
- Bestimme $s \in \{0, 1, \ldots, p-1\}$ für die $f(s)$ durch p teilbar ist. Dies sind höchstens zwei Zahlen, da das Polynom $f(X)$ höchstens zwei Nullstellen modulo p hat.
- Gehe von diesen Nullstellen aus in Schritten der Länge p im Siebintervall nach rechts und links. So werden alle $s \in S$ gefunden für die $f(s)$ durch p teilbar ist.
- Teile $f(s)$ durch die höchste Potenz von p, durch die $f(s)$ teilbar ist.
- Nachdem diese Prozedur für alle $p \in F(B)$ durchgeführt wurde, sind für genau die Zahlen, für die der Quotient 1 oder -1 bleibt, die Funktionswerte $f(s)$ B-glatt.

Beispiel 4.1.8. Fortführung
Sei $F(B) = \{2, 3, 5, 7\} \cup \{-1\}$ die Faktorbasis und $S = \{-3, -2, \ldots, 3\}$ das Siebintervall. Tabelle 4.1 zeigt das Sieb.

Tabelle 4.1: Beispiel: Quadratisches Sieb

s	-3	-2	-1	0	1	2	3
f(s)	-540	-373	-204	-33	140	315	492
Sieb mit 2	-135		-51		35		123
Sieb mit 3	-5		-17	-11		35	41
Sieb mit 5	$\boxed{-1}$				7	7	
Sieb mit 7					$\boxed{1}$	$\boxed{1}$	

Die drei Elemente -3, 1 und 2 weisen B-glatte Funktionswerte auf.
Es können nun die Kongruenzgleichungen aufgestellt werden. Es gilt:

$$\begin{aligned} f(-3) &= 83^2 - 7429 = -540 = -1 \cdot 2^2 \cdot 3^3 \cdot 5 \\ f(1) &= 87^2 - 7429 = 140 = 2^2 \cdot 5 \cdot 7 \\ f(2) &= 88^2 - 7429 = 315 = 3^2 \cdot 5 \cdot 7 \end{aligned}$$

und damit:

$$\begin{aligned} 83^2 &= -1 \cdot 2^2 \cdot 3^3 \cdot 5 \bmod 7429 \\ 87^2 &= 2^2 \cdot 5 \cdot 7 \bmod 7429 \\ 83^2 &= 3^2 \cdot 5 \cdot 7 \bmod 7429 \end{aligned}$$

In diesem Beispiel ist leicht zu sehen, dass durch Multiplikation der letzten beiden Kongruenzen auf der rechten Seite ein Quadrat entsteht. Im Folgenden soll anhand des Beispiels eine Methode aufgezeigt werden, welche auch bei einem System aus mehr als 100 000 Kongruenzen geeignete Gleichungen findet.

Auswahl geeigneter Kongruenzen

Um zwei Kongruenzen zu finden, sodass deren Produkt auf der rechten Seite ein Quadrat ergibt, sucht man Zahlen $\lambda_i \in \{0,1\}$, $1 \leq i \leq 3$, für die in der Gleichung

$$(-1 \cdot 2^2 \cdot 3^3 \cdot 5)^{\lambda_1} \cdot (2^2 \cdot 5 \cdot 7)^{\lambda_2} \cdot (3^2 \cdot 5 \cdot 7)^{\lambda_3} = (-1)^{\lambda_1} \cdot 2^{2\lambda_1 + 2\lambda_2} \cdot 3^{3\lambda_1 + 2\lambda_3} \cdot 5^{\lambda_1 + \lambda_2 + \lambda_3} \cdot 7^{\lambda_2 + \lambda_3}$$

die Exponenten aller Primzahlen sowie von der -1 gerade sind.
Es ergibt sich folgendes Kongruenzgleichungssystem:

$$\begin{aligned} \lambda_1 &\equiv 0 \bmod 2 \\ 2\lambda_1 + 2\lambda_2 &\equiv 0 \bmod 2 \\ 3\lambda_1 + 2\lambda_3 &\equiv 0 \bmod 2 \\ \lambda_1 + \lambda_2 + \lambda_3 &\equiv 0 \bmod 2 \\ \lambda_2 + \lambda_3 &\equiv 0 \bmod 2 \end{aligned}$$

Und nach Reduktion modulo 2:

$$\begin{aligned} \lambda_1 &\equiv 0 \bmod 2 \\ \lambda_1 + \lambda_2 + \lambda_3 &\equiv 0 \bmod 2 \\ \lambda_2 + \lambda_3 &\equiv 0 \bmod 2 \end{aligned}$$

Daraus ergibt sich: $\lambda_1 = 0$, $\lambda_2 = \lambda_3 = 1$. Zur Multiplikation werden also die Kongruenzen 2 und 3 genutzt. Es ist:

$$(87 \cdot 88)^2 \equiv (2 \cdot 3 \cdot 5 \cdot 7)^2 \bmod n$$

und damit

$$x = 87 \cdot 88 \bmod n = 227,\ y = 2 \cdot 3 \cdot 5 \cdot 7 \bmod n = 210.$$

Dann ist $x - y = 17$ und $x + y = 437$. Demnach ist $\mathrm{ggt}(x-y, n) = \mathrm{ggt}(17, 7429) = 17$ ein echter Teiler von $n = 7429$ und

$$n = 17 \cdot 437$$

die Faktorisierung des Moduls.
Bei einer Schranke B und einem Siebintervall S der Größenordnung $\exp\sqrt{1/2 \log n \cdot \log\log n}$ beträgt die Komplexität des Algorithmus $O(\exp\sqrt{\log n \cdot \log\log n})$ ([11], S.207).

4.1.2.2 Weitere Angriffsmöglichkeiten

Außer den Faktorisierungsangriffen gibt es, je nach Wahl der einzelnen Parameter, noch weitere Möglichkeiten, wie Eve an geheime Informationen gelangen kann. Einige davon werden im Folgenden vorgestellt.

Small Message Attack
Falls die Nachricht m und der Exponent e im Vergleich zu dem Modul n klein sind, so ist die Verschlüsselung unsicher. Falls nämlich $c = m^e < n$ gilt, so lässt sich m durch gewöhnliches Wurzelziehen, ohne Erschwerung durch das Modul, berechnen. Diesem Angriff kann allerdings leicht vorgebeugt werden, indem entweder e oder m ausreichend groß gewählt wird. Im Allgemeinen wird der Schlüssel e klein gehalten, um die Verschlüsselung zu beschleunigen.

Low Exponent Attack
Der öffentliche Schlüssel e wird meist relativ klein gehalten. Der kleinst mögliche Schlüssel ist $e = 3$. Angenommen drei Parteien benutzen den gleichen Schlüssel e, um die Nachricht m zu verschlüsseln. Sie verwenden jeweils die Module n_1, n_2 und n_3. Es entsteht folgendes Kongruenzgleichungssystem:

$$\begin{aligned} c_1 &= m^3 \bmod n_1 \\ c_2 &= m^3 \bmod n_2 \\ c_3 &= m^3 \bmod n_3 \end{aligned}$$

Eve kann mithilfe des Chinesischen Restsatzes berechnen:

$$c = m^3 \bmod n_1 n_2 n_3$$

Da $m < n_i, i \in \{1, 2, 3\}$, gilt auch $m^3 < n_1 n_2 n_3$ und damit kann Eve wieder wie bei einer *Small Message Attack* m durch einfaches Wurzelziehen berechnen.
Dieser Zusammenhang kann auf den allgemeinen Fall mit e Parteien übertragen werden. Ein solches Szenario könnte wie folgt aussehen: Eine Bank schickt an mindestens e verschiedene Kunden dieselbe Nachricht und verwendet dabei deren öffentliche Schlüssel n_i, jedoch immer denselben Schlüssel e. Der Angreifer kann dann mithilfe des Chinesischen Restsatzes und einfachem Wurzelziehen die Nachricht entschlüsseln.
Um solche Angriffe vorzubeugen, sollte e möglichst groß gewählt werden. Häufig verwendet wird z. B. $e = 2^{16} + 1$. Eine andere Möglichkeit besteht in dem Einfügen oder Anhängen von verschiedenen zufälligen Bits, um die eigentlich identischen Nachrichten unterschiedlich werden zu lassen [7], Abschnitt 7.3.7.

Angriffe aufgrund von Seiteneffekten
Paul Kocher entdeckte 1995 eine ganz andere Art des Angriffs auf Verschlüsselungssysteme. Er machte sich die Tatsache zu Nutzen, dass die Rechenzeit eines Algorithmus vom verwendeten Schlüssel abhängt. Ein Angreifer der Zugang zum

Rechnersystem hat, könnte demnach die Laufzeiten messen und daraus die einzelnen Schlüsselbits herleiten.
Auch gegen diese Methode gibt es Gegenmaßnahmen: Der Algorithmus kann so verändert werden, dass die Rechenzeiten sich einander anpassen. Eine andere Möglichkeit ist es, jeder Operation eine Warteschleife zufälliger Dauer anzuhängen, um die Rechenzeiten vollständig zu verschleiern.
Ein weiterer Seiteneffekt, der Rückschlüsse auf die Schlüsselzeichen zulässt, ist der Stromverbrauch [8], Abschnitt 5.3.1.

Chosen Plaintext Attack

Da Eve Zugang zum öffentlichen Schlüssel von Bob hat, kann sie ganz einfach verschiedene Klartexte verschlüsseln und mit dem Geheimtext von Alice vergleichen. Diese Methode ist besonders für sehr kurze Nachrichten einsetzbar. Wenn Eve dann auch noch eine Ahnung über den Inhalt der Nachricht hat, etwa dass Alice eine Ja / Nein Antwort verschickt, so hat sie recht leichtes Spiel.

Man in the Middle Attack

Bei diesem Angriff täuscht Eve Alice vor, Bob zu sein, und umgekehrt. Sie fängt Alice's öffentlichen Schlüssel e_A ab und sendet stattdessen ihren eigenen Schlüssel e_E an Bob (siehe Abbildung 4.1).



Abbildung 4.1: Man-in-the-Middle Angriff, Quelle: Eigene Darstellung nach [8], S.87

Wenn dieser eine Nachricht mit diesem Schlüssel chiffriert, so kann Eve den Geheimtext mühelos entziffern. Darüber hinaus hat sie die Möglichkeit die Nachricht zu modifizieren, sie mit Alice's öffentlichem Schlüssel zu verschlüsseln und Alice zukommen zu lassen. Alice und Bob können einen solchen Angriff vermeiden, indem sie die Authentizität der Schlüssel überprüfen [8], Abschnitt 5.4.1.

4.1.2.3 Parameter-Empfehlungen

Alle vorgestellten Angriffe auf das RSA-Verfahren resultieren in Bedingungen für die einzelnen Parameter. Zusammenfassend sollen nun die Empfehlungen zur Wahl der Primzahlen p und q, des Schlüssels e, sowie des Textes m aufgelistet werden (Karpfinger [11], S.126).

Wahl von p und q
Um Faktorisierungsangriffe unerfolgreich werden zu lassen, sollten die Primzahlen p und q unter folgenden Bedingungen gewählt werden:

- ✔ p und q haben etwa die gleiche Größenordnung, mindestens 512 Bits und
- ✔ $p-1$ besitzt einen großen Primteiler r und $q-1$ besitzt einen großen Primteiler s.

Wahl von e und d
Auch die Wahl des Schlüssels e und damit auch des geheimen Schlüssels d kann Auswirkungen auf die Sicherheit des Systems haben. Aus den vorgestellten Angriffen resultieren die Bedingungen:

- ✔ Wähle e relativ klein, um die Verschlüsselung zu beschleunigen, aber
- ✔ bei der Teilnahme von x Parteien, wähle $e > x$.

Wahl von m
Um einer *Small Message Attack* vorzubeugen, sollte die Nachricht m nicht zu klein gewählt werden.

4.2 Der Diffie-Hellman-Schlüsselaustausch

Das Verfahren von Diffie & Hellman bietet eine Möglichkeit einen gemeinsamen Schlüssel für den Gebrauch in einem symmetrischen System zu generieren. Das Entscheidende dabei ist, dass dieser Schlüsselaustausch auch über unsichere Kanäle stattfinden kann, ohne dass ein Angreifer den vereinbarten Schlüssel kennt oder berechnen kann. Das Verfahren wurde im Jahre 1976 von Whitfield Diffie und Martin Hellman veröffentlicht und patentiert ([8], S.88). Wie auch der RSA-Algorithmus, beruht dieses Verfahren auf einem mathematischen Problem, dem **Diskreten Logarithmus-Problem**, welches im Folgenden vorgestellt wird. Im Anschluss wird das Verfahren beschrieben und hinsichtlich seiner Sicherheit diskutiert. Die Ausführungen in diesem Kapitel beruhen weitestgehend auf dem Buch Kryptologie von Karpfinger und Kiechle ([11], Kapitel 9 & 10).

4.2.1 Der diskrete Logarithmus

Sei G eine zyklische Gruppe und $g \in G$ ein erzeugendes Element mit $G = \langle g \rangle$.

Definition 4.2.1. Das diskrete Logarithmusproblem (DLP)

$$\text{Gegeben ist } a \in G = \langle g \rangle, \text{ gesucht ist } x \in \mathbb{Z} \text{ mit } a = g^x.$$

Das kleinste, nichtnegative solcher x heißt *diskreter Logarithmus* von a zur Basis g. Schreibe: $x = \log_g a$.

Das Diffie-Hellman-Verfahren lässt sich auf allen Gruppen sicher durchführen, in denen die Berechnung diskreter Logarithmen schwer ist, während die Ausführung der Gruppenoperation leicht ist ([7], S.130). Das in diesem Abschnitt beschriebene Verfahren bezieht sich auf die multiplikative zyklische Gruppe $G = \mathbb{Z}_p^*$. Das Element $\bar{g} \in \mathbb{Z}_p^*$ mit $\langle \bar{g} \rangle = \mathbb{Z}_p^*$ wird Primitivwurzel modulo p genannt. Es existieren genau $\varphi(p-1)$ Primitivwurzeln modulo p.

Beispiel 4.2.2. Sei $p = 13$. Da $\text{ord}(\bar{2}) = \varphi(13) = 12$, ist $\bar{2}$ eine der $\varphi(12) = 4$ Primitivwurzeln mod 13.
Da $\langle \bar{2} \rangle = \mathbb{Z}_{13}^*$ gibt es für alle $a \in \{1, \ldots, p-1\}$ ein $x \in \{0, \ldots, p-2\}$ mit

$$a \equiv \bar{2}^x \bmod 13:$$

a	1	2	3	4	5	6	7	8	9	10	11	12
x	0	1	4	2	9	5	11	3	8	10	7	6

4.2.2 Schlüsselaustausch

Für die Anwendung eines symmetrischen Verfahrens wollen sich Alice und Bob auf einen geeigneten Schlüssel $k \in K$ einigen, ohne dass die Angreiferin Eve durch Abhören der Kommunikation an den Schlüssel gelangen kann. Der Diffie-Hellman-Schlüsselaustausch funktioniert wie folgt:

1. Alice und Bob einigen sich auf eine Primzahl p und eine Primitivwurzel g mod p.
2. Alice wählt eine natürliche Zahl $a \in \{2, \ldots, p-2\}$, bestimmt $g^a \in \mathbb{Z}_p^*$ und sendet
$$A := g^a \bmod p$$
an Bob.
3. Bob wählt eine natürliche Zahl $b \in \{2, \ldots, p-2\}$, bestimmt $g^b \in \mathbb{Z}_p^*$ und sendet
$$B := g^b \bmod p$$
an Alice.
4. Alice berechnet $B^a = g^{ab} = k$.
5. Bob berechnet $A^b = g^{ab} = k$.

Beispiel 4.2.3. Es ist $\bar{2}$ eine Primitivwurzel modulo 13.

	Schritt 1	Schritt 2 & 3		Schritt 4 & 5
Alice:	$a = 7$	$\bar{2}^7 = \bar{11}$	$\searrow$	$\bar{3}^7 = \bar{3}$
Bob:	$b = 4$	$\bar{2}^4 = \bar{3}$	$\nearrow$	$\bar{11}^4 = \bar{3}$

4.2.3 Sicherheit

Eve hört die Kommunikation zwischen Alice und Bob aus obigem Beispiel ab. Abbildung 4.2 zeigt die Informationen, die öffentlich kommuniziert werden.

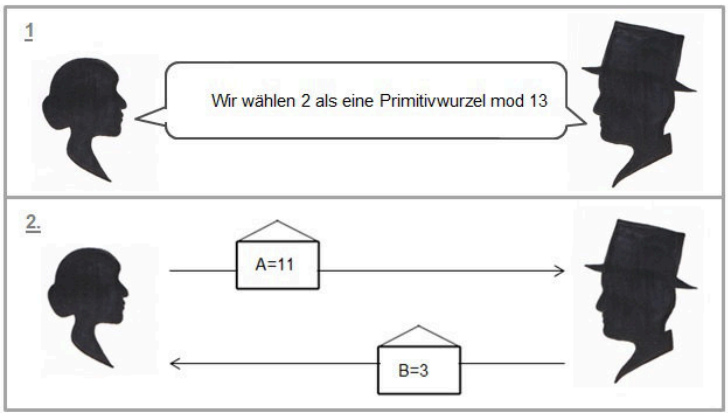


Abbildung 4.2: Diffie-Hellman-Schlüsselaustausch: Kommunikationsbeispiel, Quelle: Eigene Darstellung

Alice kann in diesem Beispiel den Schlüssel $k = g^{ab}$ ermitteln. Zu Lösen sind die beiden DLPs:

$$x_1 = \log_{\bar{2}}(\bar{11}) \bmod 13$$
$$x_2 = \log_{\bar{2}}(\bar{3}) \bmod 13$$

Durch Berechnung der Potenzen von $\bar{2}$ modulo 13 erhält sie:

$$\bar{2}^2 = \bar{4} \qquad \bar{2}^3 = \bar{8} \qquad \bar{2}^4 = \bar{3}$$
$$\bar{2}^5 = \bar{6} \qquad \bar{2}^6 = \bar{12} \qquad \bar{2}^7 = \bar{11}$$

und damit: $x_1 = 7$, $x_2 = 4$.

Allgemein formuliert gilt also: Alice kennt p, g^a und g^b und möchte daraus g^{ab} berechnen. Sie kann dieses Problem lösen, wenn sie die DLPs

$$a = \log_g(\bar{A}) \bmod p$$
$$b = \log_g(\bar{B}) \bmod p$$

berechnen kann. Die Primzahl p ist dabei so zu wählen, dass das Diskrete Logarithmusproblem schwer zu lösen ist.
Es ist bisher nicht bekannt, ob Alice den Schlüssel berechnen kann, ohne das DLP zu lösen. Im Folgenden werden exemplarisch zwei Methoden zur Lösung dieses Problems vorgestellt.
Eine weitere Gefahr besteht wiederum in dem in Abschnitt 4.1 vorgestellten Man-in-the-Middle Angriff.

4.2.3.1 Enumeration

Zur Berechnung von $x = \log_g a$ werden die Werte

$$g, g^2, g^3, \ldots$$

sukzessive berechnet, bis gilt:

$$g^i = g^x \text{ für ein } i \in \{0, \ldots, p-2\}.$$

Der Algorithmus ist mit einer Laufzeit von $O(|G|)$ wenig effizient.

4.2.3.2 Babystep-Giantstep-Algorithmus

Der Babystep-Giantstep-Algorithmus von Shanks ist eine schnelle Methode zur Berechnung des diskreten Logarithmus $x = \log_g a$.
Setze

$$n := \left\lceil \sqrt{|G|} \right\rceil$$

Damit gilt $n^2 \geq |G|$ und es ist für alle $a \in G$: $x \leq n^2$.
Division mit Rest von x durch n ergibt:

$$x = qn + r,\ r \in \{0, \ldots, n-1\},\ q \in \{0, \ldots, n\}$$

Es ist also

$$a = g^x = g^{qn+r}$$

und damit

$$ag^{-r} = g^{qn}$$

Durch Ermittlung von r und q, sodass die obige Gleichung erfüllt ist, kann also x berechnet werden. Dazu werden zwei Listen, eine für die linke Seite der Gleichung (*Babysteps*) und eine für die rechte Seite (*Giantsteps*), erstellt und die Einträge verglichen.

Babystep Liste:	ag^{-r}	$\Vert$	ag^0	ag^{-1}	ag^{-1}	$\ldots$	ag^{-n+1}
Giantstep Liste:	g^{qn}	$\Vert$	g^0	g^n	g^{2n}	$\ldots$	g^{nn}

Die Komplexität des Algorithmus beträgt $O(\sqrt{|G|})$. Er ist ab $|G| > 2^{160}$ nicht mehr einsetzbar.

Beispiel 4.2.4. Sei $G = \mathbb{Z}_{97}^* = \langle \bar{5} \rangle$, also $g = \bar{5}$ und $a = \bar{31}$. Es ist $n = \left\lceil \sqrt{|G|} \right\rceil = 10$ wegen $9^2 < |\mathbb{Z}_{97}^*| = 96 \leq 10^2$. Für $r \in \{0, \ldots, n-1\}$ und $q \in \{0, \ldots, n\}$ entstehen die beiden Listen:

Babystep Liste:	$\bar{31} \cdot \bar{5}^{-r}$	$\Vert$	$\bar{31}$	$\bar{45}$	$\bar{9}$	$\bar{60}$	$\bar{12}$	$\bar{80}$	$\bar{16}$	$\bar{42}$	$\bar{86}$	$\bar{56}$
Giantstep Liste:	$\bar{5}^{q^{10}}$	$\Vert$	$\bar{1}$	$\bar{53}$	$\bar{93}$	$\bar{79}$	$\bar{16}$	$\bar{72}$	$\bar{33}$	$\bar{3}$	$\bar{62}$	$\bar{85}$	$\bar{43}$

Für $r = 6$ und $q = 4$ ergibt sich jeweils der Eintrag $\bar{16}$ und damit ist

$$x = qn + r = 4 \cdot 10 + 6 = 46 = \log_{\bar{5}}(\bar{31})$$

5 Planung der Unterrichtsreihe

In diesem Kapitel wird zunächst die Planung der Unterrichtsreihe beschrieben, bevor in Kapitel 6 einzelne Stunden herausgegriffen und näher beleuchtet werden. Zu Beginn wird ein Bezug zum Lehrplan und den Bildungsstandards hergestellt, die Ziele der Reihe ausgearbeitet und die Bedeutung der Kryptographie als Unterrichtsgegenstand erläutert. Das Vorwissen der Schülerinnen und Schüler (SuS) wird betrachtet und im Hinblick auf Heterogenität diskutiert. Es folgt eine erste didaktische Analyse zu den möglichen Inhalten der Reihe. Das Kapitel endet schließlich mit einer tabellarischen Reihenplanung.

5.1 Lehrplan und Bildungsstandards

Der aktuelle Lehrplan des Landes Rheinlandpfalz ([17], S.7ff) für die gymnasiale Oberstufe (MSS) nennt drei wesentliche Ziele des Oberstufenunterrichts:

- Heranführung zur allgemeinen Studierfähigkeit
- Ermöglichung einer beruflichen Orientierung
- Entwicklung der Persönlichkeit in sozialer Verantwortung

Für den Mathematikunterricht ergeben sich dadurch folgende Aufgabenbereiche:

- **Mathematik im Anwendungszusammenhang:** Im Hinblick auf die allgemeine Studierfähigkeit soll den SuS die Rolle der Mathematik als Hilfswissenschaft bewusst werden. Die Anwendungsrelevanz vieler Gebiete der Mathematik soll aufgezeigt werden, um den SuS deutlich zu machen, dass die Mathematik für das Erlernen einer Vielzahl von Berufen wichtig ist. Des Weiteren soll der Prozess des Mathematisierens geübt werden, um das Zusammenspiel von Theorie und Praxis zu erfahren.
- **Mathematik als Wissenschaft:** Dem Mathematikunterricht wird hier eine wissenschaftspropädeutische Rolle zugeschrieben. Die SuS sollen einen Einblick in den strukturellen Aufbau und grundlegende Methoden der Mathematik gewinnen. Dazu gehört die Begriffsbildung und das Herausarbeiten von Definitionen, das Verstehen, Nachvollziehen und Führen von Beweisen, sowie das Erkennen von grundlegenden Leitgedanken der Mathematik.

- **Ausbildung allgemeiner geistiger Fähigkeiten und Entwicklung von Persönlichkeitsmerkmalen:** Eine Vielzahl von Persönlichkeitsmerkmalen kann und soll im Mathematikunterricht gefördert werden. Dazu gehören Fähigkeiten wie Problemlösen, Anschauungsvermögen und logisches Denken, ebenso wie Kreativität, Konzentrationsvermögen und Beharrlichkeit.

Zusätzlich zum länderspezifischen Lehrplan werden von der KMK[1] Bildungsstandards für die Allgemeine Hochschulreife formuliert, [12]. Sie legen fest, welche Kompetenzen die SuS bis zum Ende ihrer Schullaufbahn entwickelt haben sollen. Es werden folgende Kompetenzbereiche unterschieden:

- K1: Mathematisch argumentieren
- K2: Probleme mathematisch lösen
- K3: Mathematisch modellieren
- K4: Mathematische Darstellungen verwenden
- K5: Mit sybolischen, formalen und technischen Elementen der Mathematik umgehen
- K6: Mathematisch kommunizieren

Die Kryptographie als Anwendungsbereich der Mathematik wird im Lehrplan nicht erwähnt. Trotzdem bietet sie eine Fülle von Möglichkeiten, oben genannte Ziele zu verfolgen und einzelne Kompetenzen zu fördern. Besonders im Hinblick auf die Studierfähigkeit ergeben sich viele Potentiale, welche in Abschnitt 5.5 diskutiert werden. Daher ist die Unterrichtsreihe in die Zeit nach dem schriftlichen Abitur angesetzt. In dieser Zeit bis zum mündlichen Abitur herrscht oft ein gewisser „Leerlauf“: Die Inhalte des Lehrplanes sind weitestgehend abgehakt, die Motivation für reguläre Unterrichtsinhalte sinkt in zunehmendem Maße. Diese Wochen können genutzt werden, interessierten SuS einen Einblick in das Mathematikstudium zu gewähren. Die Kryptographie bietet sich hierbei hervorragend an, da sie auch für mathematisch eher uninteressierte SuS spannende Themen bereithält.

5.2 Ziele der Unterrichtsreihe

Mit dieser Unterrichtsreihe sollen grundlegend folgende Ziele verfolgt werden:

1. **Hilfe bei der Studienwahl:** SuS, die ein Mathematikstudium o.Ä. anstreben, sollen einen ersten Einblick ins Studium bekommen. Studienanfänger sind häufig nicht nur mit den neuen Methoden und Arbeitsweisen überfordert, sondern sind auch überrascht, welch großer Unterschied zwischen der Schulmathematik und der Mathematik im Studium herrscht. Diese Lücke kann

[1] Kulturministerkonferenz

nicht geschlossen, aber verkleinert werden. Die Unterrichtsreihe soll eine Einführung in die formale Mathematik darstellen. Es bietet sich die Möglichkeit, grundlegende Konzepte aus dem ersten Semester einzuführen. Welche Inhalte an welcher Stelle der Reihe möglich sind, wird in Kapitel 5.5 genauer diskutiert.

2. **Motivation:** Gegen Ende der 13. Jahrgangsstufe ist der Unterrichtsalltag im Leistungskurs darauf ausgelegt, sich auf das schriftliche Abitur vorzubereiten. Ist diese Hürde dann geschafft, bedeutet es für viele SuS das Ende der Aufmerksamkeit und des Interesses an schulischen Inhalten. Diese Unterrichtsreihe soll die Motivation noch einmal anfachen und die Zeit spannend gestalten.

3. **Schulung der Medienkompetenz:** Für die SuS ist der tägliche Umgang mit Online-Shopping und -Banking oder Social Media Plattformen etwas ganz Normales. Es ist mit die Aufgabe des Schulunterrichts die SuS zu einem kritischen Umgang mit diesen Medien zu erziehen.

5.3 Bedeutung des Unterrichtsgegenstandes Kryptographie

Die Ausführungen in diesem Abschnitt sind angelehnt an „Codierung und Kryptologie“, Borys 2011, [6].
Die Wissenschaft der Ver- und Entschlüsselung ist eine sehr alte **Kulturtechnik**. An ihrem Beispiel kann die mathematische Wissensgenese verfolgt und verstanden werden. Die Historik dieser Wissenschaft ist deshalb so wichtig, als dass sie einen wesentlichen Beitrag zur Veränderung unserer Gesellschaft von einer Industrie- zu einer **Informationsgesellschaft** leistete. Computer übernehmen in der heutigen Zeit viele Routineaufgaben.
Die **Alltagsrelevanz** der Thematik ist immens hoch. Beispiele für Kryptographie im Alltag sind:

- die menschlichen Erbanlagen als genetischer Code
- Strichcodes und Prüfsummen in Supermärkten
- Sicherheitsverfahren beim Onlinebanking / -shopping
- Verschlüsselung von E-Mails
- Verschlüsselung von Daten auf Mobiltelefonen

Die SuS kennen alle diese Anwendungen, doch die wenigsten sind sich wahrscheinlich bewusst, wie wichtig und unerlässlich die Kryptographie für sie ist. Auch die Kommunikation über das Internet nimmt stetig zu. Social-Media Plattformen wie Facebook werden von den meisten SuS genutzt.

Auch die **Berufsrelevanz** ist hoch: Nach einer Prognose von Bitcom wird bis 2030 der Software und IT-Dienstleistungssektor zu einer Schlüsselindustrie angewachsen sein. Diese Branche bietet also für die heutige Jugend vielfältige Arbeitsmöglichkeiten.

5.4 Mögliches Vorwissen aus dem Fach Informatik

Während die Kryptographie in der Schulmathematik kaum eine Rolle spielt, ist sie jedoch wesentlicher Bestandteil des Informatikunterrichts. Laut dem Lehrplan Informatik ([16]) werden kryptographische Inhalte sowohl im Grundkurs als auch im Leistungskurs im Zuge des Inhaltsbereiches „Kommunikation in Rechnernetzen" behandelt. Sowohl die historischen Verfahren als auch das Grundprinzip des RSA-Algorithmus sind Bestandteil. Abbildung 5.1 zeigt den Unterpunkt „Datensicherheit unter Berücksichtigung kryptologischer Verfahren erklären und beachten" des Grundkurses.

Datensicherheit unter Berücksichtigung kryptologischer Verfahren erklären und beachten	
Verbindliche Inhalte	**Hinweise für eine mögliche Umsetzung**
Sicherheitsziele	➢ Sicherheitsprobleme bei Kommunikationsvorgängen im Alltag aufzeigen. ➢ Die Brisanz von Sicherheitsproblemen bei elektronischer Kommunikation (z.B. Chat, E-Mail, Online-Banking, E-Vote) herausstellen und diskutieren. ➢ Vertraulichkeit, Authentizität, Integrität, Verbindlichkeit als Sicherheitsziele herausarbeiten.
Moderne Verfahren zur Verschlüsselung und Signierung	➢ Historische Verfahren nur als Anknüpfungspunkte an das Thema „Verschlüsselung" nutzen. ➢ Das Grundprinzip asymmetrischer Verfahren erarbeiten. Dabei das Prinzip der Einwegfunktion besprechen und an Beispielen verdeutlichen – die komplexen mathematischen Hintergründe der benutzten Verfahren allenfalls kurz thematisieren. ➢ Mit aktuellen Werkzeugen ver-/ entschlüsseln und signieren (z.B. GnuPG).
Sicherheitsinfrastruktur	➢ Probleme zur Sicherheitsinfrastruktur besprechen: Schlüsselvergabe, Zertifizierung von Schlüsseln. ➢ Die Grundlagen einer Sicherheitsinfrastruktur durch Austausch und gegenseitige Signierung von Schlüsseln innerhalb des Kurses aufzeigen.

Abbildung 5.1: Auszug aus dem Lehrplan Informatik, Quelle: [16]

Der Lehrplan des Leistungskurses ist lediglich im Unterpunkt „Moderne Verfahren

zur Verschlüsselung und Signierung“ durch folgende Punkte erweitert:

- Das Grundprinzip des RSA-Verfahrens erarbeiten

- Berechnungen von öffentlichen und geheimen Schlüsseln für einfache Zahlenbeispiele durchführen und Kodierungen bzw. Dekodierungen nachvollziehen

- Die Sicherheit des RSA-Verfahrens erläutern und diskutieren

Heterogenität der Lerngruppe
Die Tatsache, dass in einem durchschnittlichen Mathematik-Leistungskurs sowohl SuS mit Informatik als Grund- oder Leistungskurs als auch SuS ohne Informatik gemeinsam lernen, führt zu einer in diesem Bereich stark heterogenen Lerngruppe. Die Unterrichtsreihe ist so konzipiert, dass sie den SuS ohne Vorkenntnisse die grundlegenden Inhalte vermittelt und mithilfe geeigneter Differenzierungsmaßnamen SuS mit Vorkenntnissen gleichermaßen beansprucht. Dazu werden die Inhalte möglichst so ausgewählt, dass Überschneidungen selten sind. Dort wo sie allerdings unumgänglich sind, werden die Informatikschüler als Experten eingesetzt oder erhalten Zusatzaufgaben. Außerdem wird in dieser Reihe mehr als im Informatikunterricht die Mathematik, also beispielsweise das Definieren von Begriffen oder das Beweisen, im Vordergrund stehen. Trotzdem ist je nach Zusammensetzung und den Vorkenntnissen des Kurses vom Lehrer abzuwägen, ob ein Einsatz der Reihe, oder eine Modifikation dieser, Sinn macht. Die Abänderung macht besonders dann Sinn, wenn besonders viele oder besonders wenige Schüler Informatikunterricht hatten. Auch ist eine Absprache mit dem Informatiklehrer sinnvoll, um in Erkenntnis zu bringen, welche Inhalte genau durchgenommen wurden.
Heterogenität ergibt sich auch durch die unterschiedliche Leistungsfähigkeit der Schüler. Die Unterrichtsreihe ist, um genannte Ziele verfolgen zu können, mathematisch recht anspruchsvoll. Aufgelockert wird die Reihe jedoch durch anschauliche, leichter verständliche Phasen, um die Motivation auch bei schwächeren SuS aufrecht zu erhalten.

5.5 Analyse der Themenkomplexe

In diesem Abschnitt werden die in der Arbeit vorgestellten Inhalte hinsichtlich ihrer Einsetzbarkeit und Potentiale diskutiert. Die Themen werden nicht alle in der anschließend vorgestellten Unterrichtsreihe vorkommen, können aber Anregungen zur Anpassung der Reihe an den eigenen Unterricht geben.

Kryptographische Grundlagen

Um Kryptographie auf einem mathematisch hohen Niveau zu betreiben, sollten auch in der Schule Grundlagen gelegt werden.

- **Verschlüsselungsverfahren:** Der Begriff „Verschlüsselungsverfahren“ wird in einer Reihe zum Thema Kryptographie unumgänglich sein. Er ist anschaulich und zunächst intuitiv klar. Die mathematische Definition ist auch für SuS gut zu verstehen und eignet sich daher, um die Begriffsbildung und das Definieren zu üben. Es kann an dieser Stelle auch auf Unterscheidungen wie Block- und Stromchiffren oder Transpositions- und Substitutionsverfahren eingegangen werden. Besonders geeignet ist die Unterscheidung in symmetrische und asymmetriche Verfahren, falls im Laufe der Reihe der RSA Algorithmus oder ein Schlüsselaustauschverfahren besprochen werden soll.

- **Kryptoanalyse:** Die Kryptoanalyse ist ein spannendes Themenfeld. Je nach Verschlüsselungsverfahren ist das mathematische Niveau sehr unterschiedlich. An geeigneten Beispielen kann die Analyse dazu dienen, die historische Entwicklung der Kryptographie nachzuvollziehen: Der Fortschritt in dieser Wissenschaft beruht auf dem ständigen Entwickeln und Analysieren von Systemen. Ein weiteres Potential bietet sich hier methodisch: Die Durchführung einer Kryptoanalyse kann am PC durchgeführt werden. Die Arbeit mit dem Computer erzeugt Spannung und Motivation.

- **Perfekte Sicherheit:** Dies ist ein Thema, welches mathematisch durchaus leistbar ist. Die SuS benötigen Vorwissen aus der Stochastik, wenden also ihr Abiturwissen nochmals an. Außerdem kann der Satz von Shannon bewiesen werden.

- **Komplexitätstheorie:** Der Begriff der Komplexität kann eingeführt werden. Obwohl mit der Verwendung des Begriffs Algorithmen gut verglichen werden können, ist die Schreibweise jedoch sehr schwer verständlich. Außerdem kann hier eine sehr große und in kurzer Zeit unüberwindbare Diskrepanz zwischen Informatik- und Nichtinformatikschülern erwartet werden.

Symmetrische Verschlüsselungsverfahren

Die Behandlung der drei historischen und recht anschaulichen Verfahren stellt einen guten Einstieg in das Thema Kryptographie dar. Die jeweiligen Funktionsweisen sind für die SuS recht einfach zu verstehen. Es muss hier allerdings besonders darauf geachtet werden, dass diese Systeme vielen SuS nicht komplett neu sein werden. Dementsprechend können die Verfahren nicht nur beschrieben und geübt, sondern eine Definition des Begriffs Verschlüsselungsverfahren herausgearbeitet werden. Hier bietet sich zudem das Potential, SuS mit Vorwissen als Experten fungieren zu lassen. Des Weiteren können Unterscheidungen wie Substitutions- und Permutations- oder Block- und Stromchiffren erarbeitet werden. Um das Prinzip der Verschiebechiffre genauer beschreiben zu können, ist es an dieser Stelle angebracht, eine erste Vorstellung von Kongruenzen zu entwickeln und somit erste Studieninhalte vorzubereiten. Um einen Übergang zu asymmetrischen Verfahren zu finden, ist es sinnvoll die Angreifbarkeit symmetrischer Systeme zu erfahren und das Schlüsselaustauschproblem herauszustellen.

Public-Key-Verfahren

Die Behandlung von Public-Key-Verfahren ist in einer solchen Reihe unabdinglich. Der wissenschaftliche Fortschritt wird deutlich. Es kann herausgearbeitet werden, welchen Nutzen die Mathematik für solche Systeme hat. Für diese Reihe ergeben sich zunächst folgende Alternativen:

- **RSA-Verfahren:** Um die Behandlung des RSA-Verfahrens zu ermöglichen, ist es von Nöten, den Begriff der Restklasse zu präzisieren und die Modulorechnung zu üben. Damit wird der Umgang mit einer Thematik geschult, die vielen Studienanfängern Schwierigkeiten bereitet. Außerdem muss die Eulersche φ-Funktion eingeführt werden. Da hier einige mathematische Inhalte eingeführt werden müssen, bietet sich die Möglichkeit seitens des Lehrers, eine kleine Vorlesung zu halten. Vielen Schülern ist der Ablauf einer Vorlesung fremd; die fehlende Interaktion mit dem Dozenten erschwert das Folgen. Es kann also mit einer zeitlich und fachlich angemessenen Vorlesung gezeigt werden, was man sich unter einer solchen vorstellen darf. Im Anschluss sollte ein kleines Übungsblatt zur Bearbeitung ausgegeben werden. Diese Herangehensweise kann, je nach Schülerinteresse, positiv aber auch negativ wirken. Sie ist demnach nur bei vielen studieninteressierten SuS zu empfehlen. Die Behandlung des RSA-Verfahrens an sich verlangt wiederum einige Differenzierungsmaßnahmen für die Informatikschüler. Es besteht die Möglichkeit den Satz zur Entschlüsselung zu beweisen. Hier wäre allerdings auch die Behandlung des kleinen Satzes von Fermat notwendig. Die Angriffsmöglichkeiten auf RSA-Verfahren sind mathematisch sehr komplex.
- **Diffie-Hellman Schlüsselaustausch:** Der Diffie-Hellmann Schlüsselaustausch bietet Raum zum Modellieren. Im Mittelpunkt könnte die Frage stehen, wie man einen Schlüsselaustausch durch einen unsicheren Kanal bewerkstelligen kann. Die Thematik eignet sich dazu, Rollenspiele in der Klasse durchzuführen und an diesem Modell die Prinzipien der asymmetrischen Verschlüsselung zu entdecken. Wie auch beim RSA-Verfahren muss auch für diese Thematik das modulare Rechnen erlernt werden. Zusätzlich kann der Begriff des Erzeugers eingeführt werden.

5.6 Tabellarische Reihenplanung

In diesem Abschnitt wird ein erster Überblick über die Unterrichtsreihe gegeben. Tabelle 5.1 zeigt die einzelnen Einheiten der Reihe inklusive Thema und Inhalt. Die Einheiten sind jeweils als Doppelstunden geplant, können aber auch in zwei Einzelstunden durchgeführt werden. Die Reihe enthält eine Auswahl aus den in Abschnitt 5.5 vorgestellten Inhalten. Die einzelnen Themen wurden so gewählt, dass eine didaktisch sinnvolle Abfolge ensteht.

Stunde	**Thema**	**Inhalt**
1+2	Einführung	- Informierender Einstieg zur Reihe - Einstieg Kryptographie anhand der Thematik „NSA-Affäre“ - Fragensammlung zur Kryptographie
	Verschlüsselungsverfahren	- Historische Verfahren: Skytale, Caesar & Vigenère - Definition Verschlüsselungsverfahren
3+4	Perfekte Sicherheit	- Kryptoanalyse des Caesar Verfahrens - Definition Perfekte Sicherheit - Satz von Shannon mit Beweis
5+6	Diffie-Hellman Schlüsselaustausch	- Erarbeitung des Schlüsselaustauschs - modulares Rechnen - Angriffsmöglichkeiten

Tabelle 5.1: Unterrichtsreihenplanung

Zunächst soll eine Einführung in die Reihe bzw. das Thema Kryptographie geschehen. Anhand historischer Verfahren wird das Themenfeld eröffnet und der Begriff des Verschlüsselungsverfahrens definiert. Ein Übergang zu modernen Verfahren bietet das Thema „perfekte Sicherheit“: Die relativ einfache Kryptoanalyse des Caesar-Verfahrens wirft die Frage nach der Sicherheit auf. Neben der Definition von perfekter Sicherheit soll auch der Satz von Shannon erarbeitet und bewiesen werden. Als Paradebeispiel für perfekte Sicherheit wird das One-Time-Pad vorgestellt und an-

hand dessen das Schlüsselaustauschproblem aufgeworfen. Der Abschluss der Reihe stellt der Diffie-Hellman Schlüsselaustausch dar.
Diese Reihung stellt nur eine von vielen Möglichkeiten in diesem weiten Themenfeld dar. Sie bietet folgende Vorteile:

- **Historischer Bezug:** Sowohl historische als auch moderne Verfahren werden in der Reihe vorgestellt. Es wird deutlich, dass das Streben nach Sicherheit Antrieb zur Weiterentwicklung der Systeme war und ist. Die Entwicklung von asymmetrischen Verfahren und die Nutzung von mathematischen Problemen als entscheidende Entwicklungsschritte der Kryptographie werden deutlich.

- **Wissenschaftspropädeutik:** Die Begriffsbildung und das Beweisen werden geübt. Mit der Einführung von Restklassen, bzw. modularem Rechnen, werden erste Studieninhalte eingeführt.

- **Alltagsbezug:** Der Einstieg erfolgt an der Thematik NSA-Affäre und zeigt somit anhand schülernaher Beispiele auf, dass Kryptographie täglicher Bestandteil des Lebens ist.

- **Umgang mit Heterogenität:** Es wurde schon bei der Auswahl der Themen darauf geachtet, möglichst wenig Überschneidung mit dem Informatiklehrplan zu erzeugen. Das Thema perfekte Sicherheit ist sehr mathematisch ausgelegt. Da im Informatikunterricht meist das RSA-Verfahren als Public-Key-Verfahren vorgestellt wird, wurde sich hier bewusst für das Diffie-Hellman Schlüsselaustauschverfahren entschieden. Außerdem sorgen Zusatzaufgaben für eine angemessene Differenzierung.

6 Unterrichtsentwürfe

Die im vorherigen Kapitel vorgestellten Unterrichtsstunden werden nun im Einzelnen erläutert. Es werden jeweils Lernziele und Kompetenzen der einzelnen Stunden genannt, bevor ausführliche didaktische und methodische Analysen folgen. Verlaufspläne der einzelnen Stunden fassen das geplante Vorgehen zusammen. Im Anschluss wird jeweils das zur Durchführung der Stunden benötigte Material bereitgestellt.
Die Unterrichtseinheiten sind meist für Doppelstunden konzipiert. Je nach Stundenplan können und müssen mehrere Einheiten in zwei Einzelstunden aufgeteilt werden. Dies ist problemlos möglich. Die Bruchstelle zwischen zwei Stunden wird im Verlaufsplan als gestrichelte Linie dargestellt. Die Stunden sind für die Durchführung in einem Computerraum ausgelegt. Es wird empfohlen, einen Kursordner für den Austausch und das Bereitstellen von Dateien anzulegen.

6.1 Einführung & Verschlüsselungsverfahren

Lernziele und Kompetenzen

Grobziel: Die SuS können den Begriff des Verschlüsselungsverfahrens am Beispiel des Caesar-Verfahrens erläutern.

Feinziele:

Die SuS können...

- die Rolle der Kryptographie in unserer heutigen Gesellschaft im Hinblick auf die NSA-Affäre diskutieren
- eine Definition des Begriffs Verschlüsselungsverfahren wiedergeben
- die Durchführung der jeweiligen Verschlüsselungen anhand der Skytala, der Caesar-Scheibe und des Vigenère-Quadrates erklären
- das Caesar-Verfahren mathematisch darstellen
- ein Verschlüsselungsverfahren hinsichtlich der Bestandteile Klartext-, Geheimtext(-alphabet), Schlüssel(-menge) und Ver- bzw. Entschlüsselungsfunktion untersuchen
- die Modulo-Schreibweise im Caesar-Verfahren erläutern

Kompetenzen:

Die SuS...

- vertiefen ihre Kompetenz im mathematischen modellieren [K3], indem sie den Begriff des Verschlüsselungsverfahrens anhand von Realsituationen strukturieren und in ein mathematisches Modell übersetzen.
- schulen ihre Kompetenzen im Umgang mit formalen Elementen der Mathematik [K5], indem sie die Modulo-Schreibweise kennenlernen und erproben.
- vertiefen ihre Kompetenzen im mathematischen kommunizieren [K6], indem sie eigene Überlegungen zum Caesar- bzw. Vigenère-Verfahren strukturiert darlegen.

Didaktische Analyse

Relevanz des Gegenstandes

Der erste Unterrichtsgegenstand, die NSA-Affäre, weist eine große Gegenwarts- sowie Zukunftsbedeutung auf. Der Skandal wird aktuell diskutiert und ist regelmäßig in den Medien zu verfolgen. Es ist zu vermuten, dass sich dies so schnell nicht ändern wird. Die Affäre betrifft im Grunde auch alle Schüler direkt. Die Sammlung von Daten greift die persönlichen Rechte an. Für die Unterrichtsreihe ergeben sich folgende Potentiale: Die Rolle der Kryptographie kann in diesem Zusammenhang herausgestellt und damit diese Wissenschaft als für die heutige Zeit immens wichtig beurteilt werden.
Im Folgenden werden die drei historischen Verfahren (Skytala, Caesar- und Vigenère-Verfahren) Unterrichtsgegenstand sein. Diese Verfahren spielen in der heutigen Zeit kaum noch eine Rolle. Jedoch stehen sie exemplarisch für alle symmetrischen Verschlüsselungsverfahren, die in der Geschichte Verwendung fanden. Die historische Entwicklung der Kryptographie wird hier deutlich: Ohne diese einfachen Anfänge und deren Weiterentwicklung gäbe es keine moderne Kryptographie. Des Weiteren bietet sich ein mathematisches Potential: Im Zuge der Caesar- und Vigenère-Chiffre kann die Kongruenzschreibweise kennengelernt werden.

Struktur des Inhalts

Die Unterrichtsreihe soll mit einem Informierenden Einstieg beginnen. Um die in Abschnitt 5.2 genannten Ziele der Unterrichtsreihe erreichen zu können, ist es von Vorteil, wenn die SuS den Sinn und Zweck der Reihe erfahren. Ohne das eigentliche Thema Kryptographie zu verraten, soll den SuS bewusst werden, dass die kommenden Stunden keinen eigentlichen Schulstoff beinhalten, sondern ein spannendes Anwendungsfeld der Mathematik vorstellen werden. Diese Art der Einführung hat den Vorteil, dass die Spannung auf das Thema erhöht wird. Es soll betont werden, dass diese Reihe einen kleinen Einblick in das Mathematikstudium geben soll, ohne

die SuS mit einem anderen Studienwunsch zu vernachlässigen. Es wird erklärt, dass es während dem wie gewohnt ablaufenden Unterricht kleinere Exkurse geben wird. Der Vorteil dabei ist, dass sich bei SuS mit mathematischem Studienwunsch eine erhöhte Aufmerksamkeit einstellen wird. Auf der anderen Seite kann dies jedoch auch zu Missmut bei den anderen SuS führen. Dies soll im Gespräch verhindert werden, indem betont wird, dass die Inhalte durchaus für alle Leistungskursschüler interessant und gut zu verstehen sind.
Die Einführung in das Thema Kryptographie folgt im Anschluss. Gegenstand soll ein aktuelles Thema sein, mit dem die SuS auch schon konfrontiert wurden. Es bieten sich mehrere Möglichkeiten: Themen wie Online-Banking, Phishing Emails oder die NSA-Affäre sind aktuell und spielen auch im Alltag der SuS eine Rolle. Es kann eine gewisse Betroffenheit erzeugt werden, die in erhöhter Aufmerksamkeit und Motivation mündet. Da für die meisten SuS der NSA-Skandal im vergangenen Jahr 2013 wohl am aktuellsten im Gedächtnis geblieben ist und immernoch Schlagzeilen macht, soll der Einstieg anhand dieser Thematik erfolgen. Der Fokus soll zunächst auf den Skandal an sich gelegt werden, um das Ausmaß klarzumachen und Betroffenheit auszulösen. Der Einstieg soll wesentliche Schlagzeilen zur Affäre beinhalten und Themen ansprechen, die die SuS direkt konfrontieren: Informationen zur Überwachung von Internetkommunikation, Telefongesprächen und Kreditkarten sowie der Social Media Plattform Facebook werden eine gewisse Emotionalität bei den SuS hervorrufen. Dazu sollen den SuS verschiedene Schlagzeilen aus dem vergangenen halben Jahr gezeigt werden [19]:

- NSA sammelt Telefondaten von Millionen US Bürgern
- USA greifen mit PRISM Daten von Internetnutzern ab
- NSA erhält auch Kreditkarten-Daten
- Regierung will mehr Datenschutz für EU Bürger
- Obama: Sicherheit erfordert Kompromisse
- Facebooks Ex-Sicherheitschef arbeitet für die NSA
- OHM[1]: Verschlüssele dein Leben

Vermutlich wird es zunächst Meldungen zur NSA-Affäre an sich geben. Die SuS dürfen sich gegenseitig über den Skandal berichten, gegenseitig Wissen austauschen. Es muss damit gerechnet werden, dass der Fokus nicht sofort auf die Kryptographie fällt, sondern z. B. auf aktuelle Themen, wie die Suche nach Asyl von Edward Snowden. Dies soll durchaus zugelassen werden. Der Einstieg soll aber inhaltlich schon auf Kryptographie hinweisen. Hierzu eignet sich die Meldung eines Hacker-Camps aus den Niederlanden: „OHM: Verschlüssele dein Leben“. Die Kryptographie soll als Sicherheitsmaßnahme gegen Überwachung in das Blickfeld der SuS gerückt

[1] OHM steht für Observe, Hack, Make, ein Festival für Hacker

werden und im Zuge dessen die Bedeutsamkeit der Kryptographie in der heutigen Zeit herausgestellt werden. Nachdem das Thema der Reihe bekannt ist, soll eine Fragensammlung erarbeitet werden. Die SuS sollen somit die Möglichkeit haben, eigene Fragen und Anregungen mit in den Schulunterricht einbringen zu können. Die Fragen sollen vom Lehrer so geordnet werden, dass wenn möglich, eine Einteilung in verschiedene Rubriken wie etwa „Sicherheit“, „Geschichte“, „Analyse“ und „Verfahren“ entsteht. Die Nennung der Rubriken soll erst nach der letzten gestellten Frage geschehen, um die SuS nicht in ihrem Denken einzuengen. Die Ordnung hat den Vorteil der Übersichtlichkeit. Der Lehrer muss allerdings flexibel reagieren, falls unerwartete Fragen entstehen, die sich nicht einordnen lassen (Rubrik: „Sonstiges“). Im Anschluss soll von dem Lehrer ein kurzer Überblick darüber gegeben werden, welche Fragen im Laufe der Reihe auf jeden Fall beantwortet werden können. Auch hier ist Flexibilität gefragt: Wenn möglich, kann die Reihe um weitere interessante Punkte erweitert werden, um möglichst viele Fragen der SuS zu beantworten. Eine Möglichkeit wäre hier die Vergabe von Referatsthemen, die im Anschluss an die Reihe gehalten werden können. Abbildung 6.1 zeigt mögliche Schülerfragen in den fünf Kategorien. Die blau unterstrichenen Fragen werden in der Unterrichtsreihe beantwortet.

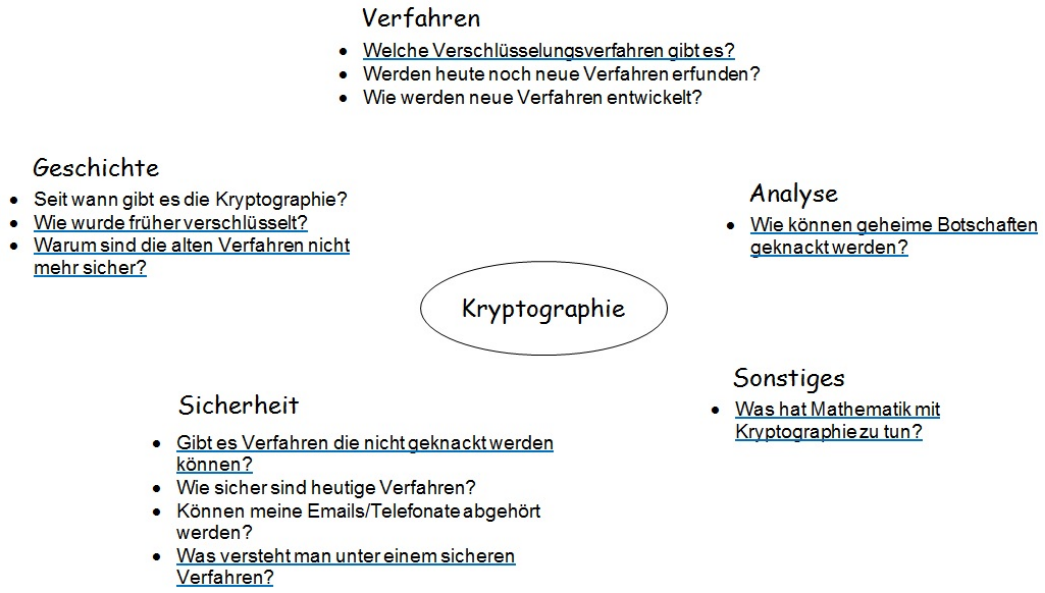


Abbildung 6.1: Beispiel für eine Fragensammlung, Quelle: Eigene Darstellung

Im Folgenden soll vom Lehrer darauf aufmerksam gemacht werden, dass der Begriff „Verfahren“ immer wieder auftaucht. Doch was versteht man eigentlich unter einem Verschlüsselungsverfahren? Die Merkmale, die zur exakten Beschreibung eines Verschlüsselungsverfahrens verwendet werden, sollen in dieser Einheit durch die SuS erarbeitet werden. Dafür stehen im Prinzip alle Arten der Verschlüsselung zur Verfügung. In dieser Stunde werden die in Kapitel 3 vorgestellten Verfahren

(Skytala, Caesar und Vigenère) aus folgenden Gründen genutzt: Die Handhabung der Verfahren ist leicht verständlich, alle drei Verfahren können anhand von „Verschlüsselungsmaschinen“ zunächst verstanden werden, bevor eine Mathematisierung stattfindet. Das Kennenlernen der Verfahren soll sich in zwei Phasen gliedern: Zunächst können diese durch SuS beschrieben werden, die die Verfahren schon kennen. Danach werden sich die SuS in Kleingruppen mit den Verfahren auseinandersetzen, die einzelnen Methoden durchsprechen und ausprobieren. Dies hat den Vorteil, dass SuS mit Vorkenntnissen in diesem Bereich als Experten fungieren können und ihren Mitschülern die Verfahren erläutern dürfen. Falls es ein Verfahren gibt, welches keiner der SuS auf Anhieb erklären kann, so dürfen Vermutungen zur Verwendung gemacht werden, bevor der Lehrer aufklärt.
Im Anschluss erfolgt die Erarbeitung der fünf Merkmale eines Verschlüsselungsverfahrens: Der Klartextraum, der Schlüsseltextraum, die Ver- und die Entschlüsselungsfunktion sowie der Schlüsselraum. Hierzu entstehen zwei Möglichkeiten der Reihenfolge: Die SuS könnten zunächst vor die Aufgabe gestellt werden, eines der Verfahren zu mathematisieren und vorzustellen. Nach der Präsentation könnten jeweils die fünf Begriffe zugeordnet werden. Hier entsteht das Problem, dass es sehr schwer ist etwas zu mathematisieren, ohne Merkmale zu kennen, auf die geachtet werden sollen. Deshalb soll die zweite Möglichkeit umgesetzt werden: Es werden zunächst die Merkmale erarbeitet und erst im Anschluss die Verfahren als Übung mathematisiert. Eine zentrale Frage soll dazu dienen das Gebilde „Verschlüsselungsverfahren“ zu erschließen: „Welche Gemeinsamkeiten / Unterschiede haben die drei Verfahren?“
Mögliche Schülerantworten sind:

- Gemeinsamkeit: Zunächst liegt ein Text vor, der mithilfe einer Vorschrift in einen verschlüsselten Text übersetzt wird.
- Gemeinsamkeit: Es muss sich auf einen Schlüssel geeinigt werden, um erfolgreich Ver- und Entschlüsseln zu können.
- Unterschied: Die Vorschrift mit der verschlüsselt wird, unterscheidet sich.
- Unterschied: Bei der Skytala ist der Umfang entscheidend, beim Caesar-Verfahren ein bestimmter Buchstabe, beim Vigenère-Verfahren ein Wort.

Im Anschluss werden die Antworten zusammengetragen. Dabei werden wieder ähnliche Antworten vom Lehrer gebündelt. Danach sollen von den SuS Überbegriffe zu den einzelnen Schwerpunkten / Merkmalen gefunden werden.
Nun erfolgt die Definition des Begriffs. Diese wird vom Lehrer in Zusammenarbeit mit den SuS erstellt. Eine mögliche Endversion könnte wie folgt aussehen:

Definition: Verschlüsselungsverfahren

Die Menge A sei eine Zeichenmenge. Ein Verschlüsselungsverfahren besteht aus:

(i) Dem Klartextraum $M \subseteq A^n$, $n \in \mathbb{N}$,

(ii) dem Geheimtextraum $C \subseteq A^n$,

(iii) dem Schlüsselraum K,

(iv) der Verschlüsselungsfunktion $E_k : M \to C$ und

(v) der Entschlüsselungsfunktion $D_k : C \to M$.

Außerdem gilt:

(vi) Für jedes $e \in K$ gibt es ein $d \in K$, sodass für alle $m \in M$ die Gleichung

$$D_d(E_e(m)) = m$$

gilt.

Im Gegensatz zu Definition 2.1.3 wurde hier auf den Begriff Alphabet verzichtet und stattdessen eine Zeichenmenge eingeführt. Würde man stattdessen Alphabet schreiben, so wären die SuS zu fixiert auf das Alphabet $A - Z$. Außerdem wurde die Nachrichtenlänge fixiert und statt Mengen von Ver- und Entschlüsselungsfunktionen nur jeweils eine Funktion angegeben. Trotzdem muss diese Definition im Anschluss ausführlich besprochen und die Schreibweisen erläutert werden.
Im Anschluss erfolgt der Prozess des Mathematisierens des Caesar-Verfahrens. Hier wird sich auf dieses Verfahren beschränkt, um einen einheitlichen Lernerfolg der ganzen Gruppe zu gewährleisten. Würden auch Skytala und das Vigenère-Verfahren in Gruppen weiter behandelt werden, so ergäben sich folgende Probleme: Die Bearbeitung der verschiedenen Verfahren ist unterschiedlich anspruchsvoll. Die zeitlichen Unterschiede wären zu groß. Außerdem entsteht bei der Caesar- und der Vigenère-Verschlüsselung das Problem, dass die SuS die Kongruenzschreibweise noch nicht kennen. Die SuS sollen bewusst vor dieses Problem gestellt werden, um die Notwendigkeit der Erarbeitung der neuen Schreibweise herauszustellen. Dieser Lernerfolg kann nur bei allen SuS gleichermaßen erzielt werden, wenn sich alle Gruppen mit dem Caesar- oder dem Vigenère-Verfahren auseinandersetzen. Da das Caesar-Verfahren didaktisch der Vorgänger des Vigenère-Verfahrens darstellt, wird dies Inhalt der Aufgabe sein. Die erste Schwierigkeit ergibt sich dabei, das Alphabet durch die Zahlen $0 - 25$ oder alternativ $1 - 26$ zu repräsentieren. Diese Information kann zur Not als Hilfestellung vom Lehrer gegeben werden, falls sich manche Gruppen zu schwer damit tun. Hier zeigt sich wieder der Vorteil des Begriffs „Zeichenmenge“ in der Definition des Verschlüsselungsverfahrens. Als Differenzierungsmaßnahme eignet sich das Vigenère-Verfahren. Nachdem das Caesar-Verfahren mathematisiert wurde, führen Abwandlungen zum Vigenère-Verfahren. Es wird nicht erwartet, dass

das Verfahren exakt mathematisch dargestellt wird. Vermutlich entstehen aber bei den leistungsstarken Schülern gute Ideen zur Umsetzung. Bei der Besprechung der Aufgabe 3 soll also auch das Problem der Darstellung der Addition über den Buchstaben Z hinaus herausgestellt werden. Da es einige SuS geben wird, die schon aus dem Informatikunterricht mit der Kongruenzschreibweise vertraut sind, haben diese dann die Möglichkeit ihren Mitschülern den Sachverhalt zu erklären. Dazu sind geeignete methodische Hilfsmittel bereitzustellen. Zu diesem Zeitpunkt der Reihe soll also ein erster Kontakt mit der Kongruenzschreibweise erfolgen, ohne eine tiefere mathematische Definition zu liefern. Um das Verständnis zu überprüfen, wird die Uhrzeit als zweite Anwendung dieser Schreibweise aufgezeigt. Ein Schüler, der bislang noch nicht mit der Schreibweise in Verbindung gekommen ist, darf sich an einer Erklärung versuchen und einfache Kongruenzgleichungen wie z. B. $2 \equiv 14 \bmod 12$ aufschreiben.

Methodische Analyse

Die Einführung in die Unterrichtsreihe wird durch einen informierenden Vortrag durch den Lehrer stattfinden. Im Anschluss soll die Aufmerksamkeit auf den NSA-Skandal geleitet werden. Dazu sollen den SuS verschiedene Schlagzeilen aus dem vergangenen halben Jahr gezeigt werden (siehe [19]). Diese könnten auf verschiedene Weisen präsentiert werden: Eine Sammlung der Schlagzeilen auf einer OHP-Folie hätte den Vorteil, dass alle Schlagzeilen auf einmal betrachtet werden können. Im Gegensatz dazu, kann bei einer Powerpoint-Präsentation die Reihenfolge der Schlagzeilen vom Lehrer gewählt und der Fokus gegen Ende auf das Thema Kryptographie geleitet werden. Außerdem erzeugt eine solche Präsentation Spannung (siehe Anhang C) und es kann ebenfalls eine zusammenfassende Folie geben, auf welcher alle Schlagzeilen zu sehen sind. Die Einführung soll als stummer Impuls auf die SuS wirken. Wenn möglich, soll eine Schülerdiskussion entstehen, die ohne ein Eingreifen des Lehrers abläuft. Der Lehrer wirft dazu dem ersten Schüler einen kleinen Gummiball zu, statt ihn wie üblich aufzurufen. Dieser Impuls reicht aus, um den SuS die Regeln der Diskussion klarzumachen: Wer den Ball in den Händen hält, darf reden und wirft ihn im Anschluss zum nächsten Redner. Um die Richtung der Diskussion zu beeinflussen, kann, wenn nötig, auf die nächste Folie umgeschaltet werden, auf der nur die Warnung „Verschlüssele dein Leben“ zu lesen ist. Auch dies soll vom Lehrer unkommentiert bleiben.
Nachdem die Kryptographie als das Thema der folgenden Stunden herausgestellt wurde, erfolgt die Erarbeitung der Fragensammlung. Dies kann als eine Art Mind Map an der Tafel oder am PC geschehen. Die SuS nennen ihre Frage, der Lehrer notiert und sortiert diese. Man könnte die Fragen von den SuS an der Tafel anschreiben lassen, dies hätte jedoch den Nachteil, dass der Lehrer die Fragen nicht nach Rubriken ordnen kann. Geeigneter ist die Fragensammlung am PC. Der Lehrer kann die Fragen leicht bündeln und verschieben und im Anschluss das Dokument speichern. Dies ist in diesem Fall besonders sinnvoll, da die Sammlung so die ganze Reihe begleiten kann. Die Datei „Fragensammlung.docx“ (siehe Anhang C) ist dazu

geeignet, Fragen gebündelt zu notieren. Die Überschriften werden erst nach Ausfüllen durch Änderung der Farbe sichtbar gemacht. Vom Lehrer wird im Anschluss darauf hingewiesen, welche Fragen in der Reihe beantwortet werden und eventuell Referate verteilt.
Es folgt die Erarbeitung der drei Verschlüsselungsverfahren. Dazu werden vom Lehrer die drei Verschlüsselungsmaschinen auf dem Pult präsentiert (siehe Abbildung 6.2). Auch dies wirkt wieder als stummer Impuls. Einzelne SuS dürfen nach vorne kommen, um Vermutungen über die Handhabung zu erklären. Alternativ könnten Bilder der einzelnen Maschinen gezeigt werden. Diese mitzubringen hat jedoch einige Vorteile: Anschaulichkeit, Erzeugung von Aufmerksamkeit und Motivation.

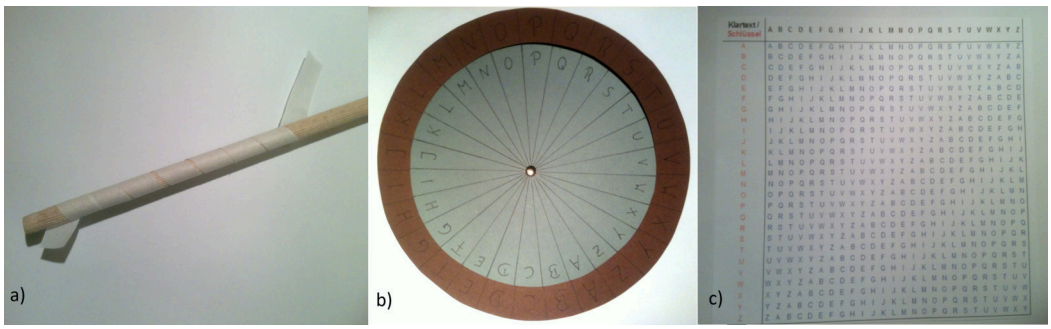


Abbildung 6.2: Verschlüsselungsmaschinen: a) Skytala von Sparta b) Caesar-Scheibe [2] c) Vigenère-Quadrat [2] Quelle: Eigene Darstellung

Im Anschluss sollen Gruppen gebildet werden. Pro Gruppe ist es sinnvoll, alle drei Verschlüsselungsmaschinen einmal zur Verfügung zu stellen. Am geeignetsten sind hierbei Dreiergruppen, was aber auch den materiellen Aufwand maximal werden lässt. Alternativ können sich je zwei Gruppen das Material teilen. Es werden Arbeitsblätter ausgegeben, auf denen zunächst zwei Aufträge bearbeitet werden sollen (siehe Material AB 1). Vom Lehrer ist darauf hinzuweisen, dass zunächst nur die Aufgaben 1 und 2 bearbeitet werden sollen. Es folgt die Zusammentragung der Ergebnisse an der Tafel. Die Überbegriffe, die von den SuS gefunden werden, können auf laminierte Karten geschrieben und mit Magneten den einzelnen Bereichen der Tafel zugeordnet werden. Es ist darauf zu achten, dass eine Seite der Tafel frei bleibt, um später die Definition notieren zu können, ohne den Blick auf die zusammengetragenen Merkmale zu verhindern. Die SuS notieren die Definition auf dem Arbeitsblatt und wenden sich dann Aufgabe 3 wieder in Gruppenarbeit zu.

[2] Im Internet gibt es zahlreiche Druckvorlagen, die zur Erstellung von Caesar-Scheiben hilfreich sein können.

Die Gruppenergebnisse, sowie die Ergebnisse der Zusatzaufgabe, werden im Anschuss auf Folie präsentiert und verglichen. Da die Modulo-Schreibweise an dieser Stelle durch einen Schüler erfolgen soll, sind geeignete Hilfsmittel zur Erklärung bereit zu stellen. Es eignet sich das Schaubild in Abbildung 6.3. Im Anschluss wird ein ähnliches Schaubild für das Rechnen modulo 12 gezeigt. Ein weiterer Schüler wird dazu aufgefordert, passende Kongruenzgleichungen an der Tafel aufzuschreiben.

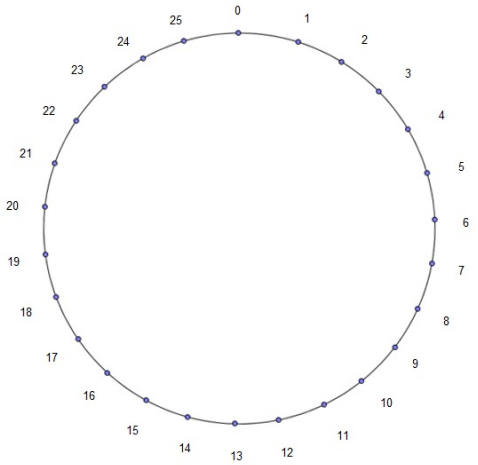


Abbildung 6.3: Visualisierungshilfe für das Rechnen modulo 26, Quelle: Eigene Darstellung

Verlaufsplan

Phase	Inhalt	UV[3]	Medien	Zeit
Einführung der Reihe	Informierender Einstieg über die Ziele der folgenden Stunden	LV		3 min
Einführung Kryptographie	- Diskussion über NSA-Affäre - Bedeutsamkeit der Kryptographie in der heutigen Zeit - Entwicklung einer Fragensammlung	SG, UG	Gummiball, Beamer, PPP[4], PC, Datei „Fragensammlung.docx“	15 min
Problemstellung	Was versteht man mathematisch gesehen unter einem Verschlüsselungsverfahren?		Tafel	2 min
Erarbeitung 1	- Beschreibung der Verfahren - Bearbeitung A1, A2 - Zusammentragen der Ergebnisse - Zuordnen von Überbegriffen	GA, UG	Verschlüsselungsmaschinen, Arbeitsblatt AB 1, Tafel, Merkmalskarten	30 min
Sicherung 1	Definition: Verschlüsselungsverfahren	UG	Tafel, Arbeitsblatt AB 1	5 min
Erarbeitung 2	Mathematisierung Caesar-Verfahren	GA	Verschlüsselungsmaschinen, AB 1, Folie	20 min
Sicherung 2 + Exkurs	- Vorstellung der Ergebnisse - Exkurs: Kongruenzschreibweise	SV	Overheadprojektor, Abbildung 6.3 auf Pappe	15min

Tabelle 6.1: Tabellarischer Verlaufsplan Einheit 1

[3] Unterrichtsverfahren - Die Abkürzungen stehen für: LV - Lehrervortag, SG - Schülergespräch, UG - Unterrichtsgespräch, GA - Gruppenarbeit, SV - Schülervortrag
[4] Powerpoint-Präsentation

Material

Arbeitsblatt 1

Datum:	**Verschlüsselungsverfahren**	Kryptographie AB 1



Das Ziel der heutigen Stunde ist es, Verschlüsselungsverfahren genauer charakterisieren zu können.

A1 Wiederholt in eurer Gruppe die Funktionsweisen der Verschlüsselungsverfahren. Verschlüsselt euch gegenseitig kurze Nachrichten und versucht diese wieder zu entschlüsseln.

A2 Diskutiert und macht euch Notizen:
Welche Gemeinsamkeiten / Unterschiede haben die drei Verfahren?

Definition: Verschlüsselungsverfahren
Die Menge A sei eine Zeichenmenge. Ein Verschlüsselungsverfahren besteht aus:

i)

ii)

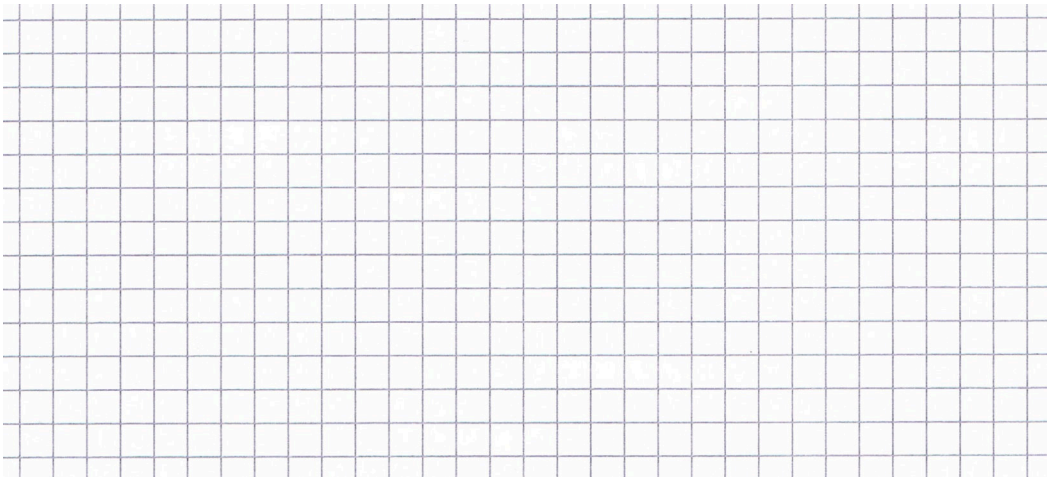
iii)

iv)

v)

vi)

A3 Stellt das Caesar Verfahren mathematisch dar, indem ihr die in der Definition gegebenen Mengen A und K, sowie die Ver- und Entschlüsselungsfunktionen angebt. Überprüft außerdem die Eigenschaft vi). Präsentiert eure Ergebnisse auf einer Folie.





Das Vigenère Verfahren ähnelt dem Caesar Verahren sehr. Der Unterschied liegt in der Schlüssellänge. Wie würde die mathematische Umsetzung dieses Verfahrens aussehen?

6.2 Perfekte Sicherheit

Lernziele und Kompetenzen

Grobziel: Die SuS können erläutern, was in der Kryptographie unter perfekter Sicherheit zu verstehen ist.

Feinziele:

Die SuS können...

- eine Definition von perfekter Sicherheit nennen
- den Satz von Shannon korrekt wiedergeben und die Rückrichtung mithilfe eines Beweispuzzles beweisen
- erklären, weshalb das Caesar-Verfahren nicht als perfekt sicher betrachtet werden kann
- das Prinzip der Kryptoanalyse des Caesar-Verfahrens beschreiben
- ein Verschlüsselungsverfahren auf perfekte Sicherheit hin untersuchen
- erläutern, weshalb das One-Time-Pad als perfekt sicher gilt

Kompetenzen:

Die SuS...

- vertiefen ihre Kompetenz im mathematischen argumentieren [K1], indem sie den Beweis des Satzes von Shannon mithilfe eines Beweispuzzles durchführen und eigenständige Begründungen liefern.
- schulen ihre Kompetenzen im Umgang mit symbolischen Elementen der Mathematik [K5], indem sie die Index-Schreibweise der verschiedenen Wahrscheinlichkeitsverteilungen verstehen und anwenden.
- vertiefen ihre Kompetenzen im mathematischen kommunizieren [K6], indem sie eigene Bedingungen formulieren, unter welchen ein System perfekt sicher ist.

Didaktische Analyse

Relevanz des Gegenstandes

In der Kryptographie und auch im Zuge dieser Reihe wird oft von Sicherheit gesprochen. In der Einführung wurde über sichere Verbindungen, Emails etc. diskutiert, ohne den Begriff näher zu spezifizieren. Dabei ist die intuitive Vorstellung über

Sicherheit nicht ausreichend. In der Mathematik ist es notwendig, verwendete Begriffe genau zu definieren. Um den SuS das Wesen der Mathematik näher zu bringen, muss Begriffsbildung also auch im Mathematikunterricht einen großen Stellenwert erhalten.
Weiterhin zeigt dieser Gegenstand die Notwendigkeit von ständigem Fortschritt auf. Als ehemals sicher geltende Verschlüsselungen sind nach einiger Zeit gebrochen worden. Um in der heutigen Zeit nicht seine ganze Identität preizugeben, sind sichere Systeme immens wichtig. Seit Beginn dieser Wissenschaft ist das oberste Ziel der Kryptographie daher die Sicherheit.

Vorwissen

Für diese Unterrichtsstunde ist besonderes Vorwissen aus dem Bereich Stochastik wichtig. Folgende Begrifflichkeiten müssen bekannt sein:

- Die bedingte Wahrscheinlichkeit: Hierbei ist auf eine einheitliche Schreibweise zu achten. Die Materialien in dieser Planung verwenden die Schreibweise "$P(B|A)$" für die durch A bedingte Wahrscheinlichkeit von B. Je nach Schulbuch kennen die SuS hierfür die Schreibweise $P_A(B)$ (siehe z.B. Lambacher Schweizer, [22], S.15).
- Stochastische Unabhängigkeit
- Satz von Bayes
- Wahrscheinlichkeitsverteilung und Gleichverteilung

Struktur des Inhalts

Um die Notwendigkeit des Themas „perfekte Sicherheit" aufzuzeigen, soll zunächst ins Bewusstsein gerückt werden, dass die bisher behandelten Systeme nicht sicher sind. Anschließend kann die Frage aufgeworfen werden, was man unter perfekter Sicherheit zu verstehen hat. Da, wie in Kapitel 3 beschrieben, alle der drei behandelten Verfahren von einem Angreifer zu brechen sind, eignen sich im Grunde alle dafür, Gegenstand der Einführungsphase zu sein. Es könnten also in Gruppen alle drei Verfahren hinsichtlich deren Analyse betrachtet werden. Allerdings ist hier der Schwierigkeitsgrad, mehr noch als bei dem Verschlüsseln an sich, sehr unterschiedlich. Besonders die Kryptoanalyse des Vigenère-Verfahrens ist sehr kompliziert und verlangt die Vorkenntnis der Analyse des Caesar-Verfahrens. Aus diesem Grund soll für alle SuS das gleiche Verfahren Gegenstand sein. Das Caesar-Verfahren eignet sich hierfür am Besten, da es für alle SuS schon in der letzten Stunde in den Fokus gerückt wurde und damit womöglich das geläufigste Verfahren ist. Außerdem ist das Prinzip der Häufigkeitsanalyse leicht verständlich. Ein weiterer Vorteil ist, dass, durch die Behandlung der Häufigkeitsanalyse, die Wahrscheinlichkeitsrechnung hier schon ins Bewusstsein gerückt wird. Mit einem PC-Tool sollen die SuS

zunächst eigene Nachrichten verschlüsseln und, ohne den Schlüsselbuchstaben anzugeben, ihrem Nachbarn zukommen lassen. Dieser soll wiederum diesen Text von einem Programm knacken lassen. Ein geeignetes Programm soll so konzipiert sein, dass die Analysewege nachvollzogen werden können. Dies soll von den SuS getan werden. Alternativ könnte man den SuS eine Anleitung zum Knacken geben. Dies würde jedoch viel mehr Zeit in Anspruch nehmen und den entdeckenden Charakter verschwinden lassen. Trotzdem soll ein geeignetes Hilfsmittel zur Verfügung stehen, anhand dessen die Häufigkeitsanalyse nachvollzogen werden kann. Hierzu eignet sich eine schriftliche Hilfe. Im Anschluss wird von den SuS kurz zusammengetragen, welche Prinzipien der Analyse zugrundeliegen. Auf eine gemeinsame Sicherung des Verfahrens wird verzichtet, da alle SuS ihre Notizen haben, die sie vervollständigen oder berichtigen können und Zugriff auf die oben erwähnte Hilfe haben. Es wird herausgestellt, dass das Caesar-Verfahren, zumindest in der heutigen Zeit, sehr unsicher ist. Doch was bedeutet es, wenn ein Verfahren als sicher gilt? Durch diese Frage wird vom Lehrer das Thema der heutigen Stunde bekanntgegeben. Die SuS werden dazu aufgefordert, Vorschläge zu unterbreiten, was unter dem Begriff perfekte Sicherheit verstanden werden könnte. Diese werden gesammelt. Es ist zu erwarten, dass die Antworten sich alle ähneln, etwa von der Art:

- Das Verfahren darf von Angreifern nicht gebrochen werden können.
- Das Verfahren darf zu 99% iger Wahrscheinlichkeit nicht gebrochen werden können.

Die SuS werden vorraussichtlich mit einer solchen Aussage zufrieden sein. Mit der Frage: „Wie weiß man denn, dass ein Verfahren nicht gebrochen werden kann?“ sollen die SuS auf das Problem aufmerksam werden, dass ein Beweis einer solchen Aussage sehr schwer ist. Wir brauchen also eine exaktere Definition der perfekten Sicherheit. Der Lehrer definiert darauffolgend ein perfekt sicheres Verfahren als ein Verfahren bei dem gilt: $P(m|c) = P_M(m)$ für alle $m \in M$ und $c \in C$. Die Aussage soll im Anschluss von den SuS erklärt werden.
Als nächster Schritt sollen die Bedingungen erarbeitet werden, unter denen ein Verfahren perfekt sicher ist. Dazu eignet es sich, ein relativ einfaches Verfahren zu formulieren, bei welchem die Ausgangswahrscheinlichkeiten und die Zuordnungsvorschrift leicht verändert werden kann. Der Satz von Shannon kann so entdeckt werden, indem die SuS versuchen, das System perfekt sicher zu machen und dann die Bedingungen unter denen es gelungen ist, selbst formulieren. Im Anschluss soll der Satz von Shannon ausformuliert und bewiesen werden. Würde die Formulierung gemeinsam in der Klasse stattfinden, so müssten an dieser Stelle Differenzierungsmaßnahmen bereitgestellt werden, um schnellere SuS nicht unbeschäftigt zu lassen. Da sich aber vor allem nach dem Beweis besondere Differenzierungsmaßnahmen bieten, soll die Formulierung des Satzes für alle SuS zeitlich individuell machbar sein. Der Satz ist also vom Lehrer vorformuliert und geeignet didaktisch reduziert bzw. vereinfacht:

Satz von Shannon
Sei $|C| = |K|$ und $P_M(m) > 0$ für alle $m \in M$. Das Verschlüsselungsverfahren ist genau dann perfekt sicher, wenn gilt:

(i) Die Schlüssel sind gleichverteilt.

(ii) Für jedes Paar (m, c) existiert genau ein Schlüssel k für den gilt: $c = E_k(m)$.

Die SuS werden aufgefordert, die eigenen Bedingungen mit dem Satz von Shannon zu vergleichen und somit die eigenen Überlegungen zu reflektieren. Es stellt sich die Frage, ob vor der Behandlung des Satzes von Shannon eine kurze Wiederholung zum Thema Wahrscheinlichkeitsrechnung stattfinden sollte. Dies hätte zum Vorteil, dass die Verteilungen der Klartexte, Geheimtexte und Schlüssel mit ihrer Indexschreibweise eingeführt werden kann. Außerdem können hier schon Grundlagen für den späteren Beweis gelegt werden. Es ergeben sich aber auch Nachteile: Der Unterrichtsfluss würde durch eine Wiederholung gestört. Außerdem ist eine Definition der einzelnen Verteilungen nicht zwingend notwendig, ein intuitiver Gebrauch reicht hier aus. Es wird daher auf eine spezifische Einführung verzichtet. Stattdessen sollen die Verteilungen mit der Indexschreibweise innerhalb der Satzfindungsphase gebraucht und erklärt werden. Die Begrifflichkeiten werden so bei den SuS eingeführt ohne zuviel Zeit einzunehmen.
Es soll die Rückrichtung bewiesen werden, da diese methodisch einfacher ist. Für alle SuS stehen Beweispuzzle als Hilfen zur Verfügung. Zunächst soll im Satz von Shannon markiert werden, welche Aussagen die Behauptung und welche die Voraussetzung darstellen. Die Begründungen für die einzelnen Schritte sollen von den SuS selbstständig gegeben werden. Abbildung 6.4 zeigt das Beweispuzzle mit vollständigen Begründungen.

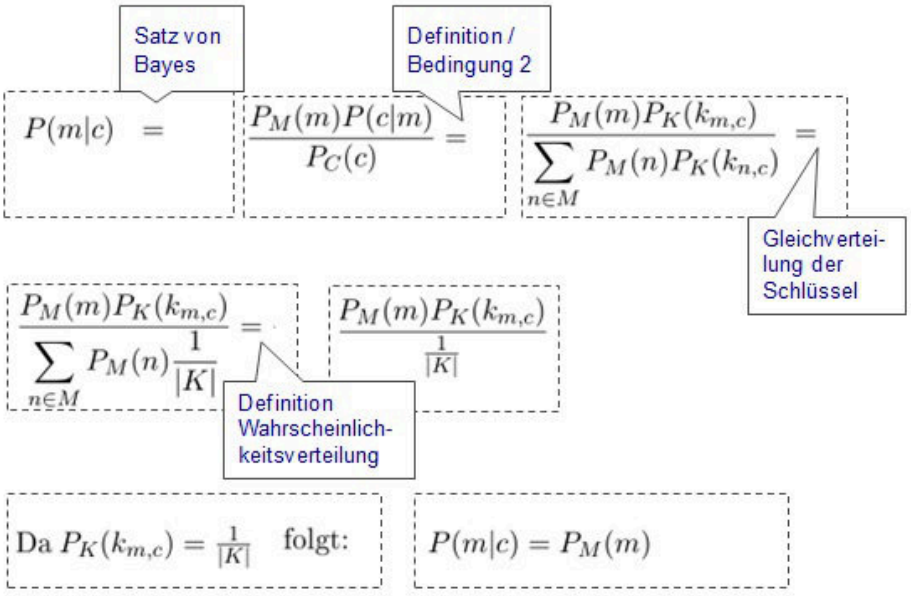


Abbildung 6.4: Beweispuzzle mit Begründungen, Quelle: Eigene Darstellung

Die Begründungen sind, vor allem wegen des Wegfalls einer Stochastikwiederholung, relativ schwer. Eine Sicherung ist unabdinglich und soll zusammen mit der Besprechung der weiteren Aufgaben am Ende der Stunde erfolgen.
Um nochmals ein perfekt sicheres Verfahren kennenzulernen und die Anwendung des Satzes von Shannon zu üben, soll das One-Time-Pad behandelt werden. Die SuS sollen Informationen zu der Funktionsweise sammeln. Die größte Schwierigkeit stellt hier die binäre Addition dar, welche nur teilweise von den SuS als bekannt vorauszusetzen ist. Eine weitere Aufgabe besteht darin, mithilfe des Satzes von Shannon zu begründen, dass, oder in welchen Fällen, das One-Time-Pad perfekt sicher ist. Eine erste Zusatzaufgabe bezieht sich in versteckter Weise auf das One-Time-Pad, der Bezug zum Caesar-Verfahren wird noch einmal hergestellt: „Wie müsste das Caesar-Verfahren verändert werden, um perfekte Sicherheit zu gewähren?“. Nach der Behandlung des One-Time-Pads kann erwartet werden, dass die SuS ein ähnliches Schema entwickeln, in welchem die Schlüsselbuchstaben in zufälliger Reihenfolge für jeweils nur einen Klartextbuchstaben fungieren. Der Beweis der Hinrichtung dient einer zweiten Differenzierung. Es wird nicht erwartet, dass ein Schüler die Richtung alleine beweisen kann. Deshalb wird sich hier zunächst auf die Frage nach einer Beweisidee beschränkt. Interessierte SuS dürfen sich den Beweis dann durchlesen (siehe Datei „Beweis.pdf“ in Anhang C).

Methodische Analyse

Die Einführung der Stunde wird am PC stattfinden. Den SuS soll bewusst werden, dass das Caesar-Verfahren leicht zu brechen ist. Dazu wird ein Arbeitsblatt ausgeteilt. Die SuS werden aufgefordert in Partnerarbeit zu arbeiten. Verwendet wird das Programm CrypTool[3]. Hiermit soll jeder Schüler eine kurze Nachricht mit einem geheimen Schlüsselbuchstaben verschlüsseln lassen und den Geheimtext dem Partner zukommen lassen. Dies geschieht am einfachsten durch Abspeichern der Datei im Kursordner, adressiert an den jeweiligen Nachbarn. Dieser öffnet wiederum die Datei mit CrypTool und lässt diese analysieren. Das Programm CrypTool eignet sich für diese Analyse sehr gut, da es mittels Häufigkeitsanalysen arbeitet. Es öffnen sich drei Fenster, anhand derer Vermutungen über den Vorgang der Analyse erfolgen können: Die Häufigkeitsverteilungen der Buchstaben aus dem analysierten Dokument sowie der deutschen Sprache werden angezeigt. Als drittes öffnet sich ein Fenster, dass die Korrelationen der beiden Verteilungen bei allen 26 Verschiebungen anzeigt. Als Hilfestellung eignet sich hierbei die Internetseite von CrypTool [9]: Auf ihr wird die Häufigkeitsanalyse direkt erklärt. Der Link dazu steht den SuS in einer Datei „Hilfe.docx“ im Kursordner zur Verfügung.
Im Anschluss sollen die Ergebnisse vorgestellt werden. Dazu wird das Programm vom Lehrer PC mit dem Beamer an die Wand projiziert werden. Ein Schüler darf also seine Nachricht öffnen und den Analysevorgang zeigen. Seine Aufgabe ist es, mithilfe des Programms, das Prinzip der Häufigkeitsanalyse zu erklären.

[3] Das Programm steht unter http://www.cryptool.org/de/ als kostenloser Download zur Verfügung.

Die anschließende Sammlung zum Thema perfekte Sicherheit wird vom Lehrer an der Tafel erstellt. Im Unterrichtsgespräch soll die Notwendigkeit einer exakten Definition des Begriffs herausgestellt werden. Diese erfolgt an der Tafel. Sie wird auf dem nächsten Arbeitsblatt AB 3 notiert sein, sodass ein Mitschreiben seitens der SuS nicht nötig ist. Die Entdeckung des Satzes von Shannon erfolgt mithilfe einer Excel Tabelle (siehe Anhang C). Die SuS erhalten das AB 3. Ihre Aufgabe ist es, das Verfahren welches in der Excel Tabelle gegeben ist, so zu verändern, dass ein perfekt sicheres Verfahren entsteht. Veränderbar sind die Wahrscheinlichkeiten der Klartextbuchstaben und der Schlüssel, sowie die Zuordnungstabelle. Angezeigt werden außerdem die Wahrscheinlichkeiten der Geheimtextbuchstaben sowie die benötigten bedingten Wahrscheinlichkeiten. Die Vermutungen der SuS werden auf dem Arbeitsblatt eingetragen.
Die Satzformulierung soll zeitlich individuell stattfinden können. Dazu dürfen sich die SuS am Pult weitere Materialien holen. Dazu gehören: Der ausformulierte Satz von Shannon und das Beweispuzzle zur Rückrichtung. Der Satz soll gelesen, eingeklebt und nachvollzogen werden. Die Aufgabe zum One-Time-Pad wird eine Recherche-Aufgabe sein. Da die Reihe in einem PC-Raum stattfindet, bietet sich diese Möglichkeit an. So kann jeder Schüler Informationen sammeln, die seinem Interesse und Verständnis entsprechen. Alternativ könnte man ein Arbeitsblatt gestalten, auf welchem das One-Time-Pad erläutert wird. Dies würde allerdings die Eigenständigkeit der SuS einschränken. Außerdem ist zu erwarten, dass auch in diesem Bereich die Diskrepanz im Kurs sehr hoch ist und somit eine eigene Recherche jedem Schüler gerecht wird. Die Sicherung dieser Phase findet mithilfe des Projektors statt. Dazu sollte das Beweispuzzle auf Folie verfügbar sein. Außerdem sollte ein Abreißblock mit Schlüsselbits vorbereitet sein, anhand dessen das One-Time-Pad erklärt werden kann. Gruppen, welche an einer Zusatzaufgabe arbeiten, bekommen noch während der Arbeitsphase Folien zur Verfügung, um ihre Ergebnisse später präsentieren zu können. Das perfekt sichere Caesar-Verfahren wird mit dem One-Time-Pad in Verbindung gebracht, indem ein leerer Abreißblock mit Caesar-Schlüsseln beschriftet wird.

Verlaufsplan

Phase	Inhalt	UV	Medien	Zeit
Einführung	- Kryptoanalyse des Caesar-Verfahrens - Das Verfahren kann mit einer Häufigkeitsanalyse leicht gebrochen werden	PA[1] UG	PC, CryptTool, Datei „Hilfe.docx“	20 min
Erarbeitung 1 / Sicherung 1	- Hyptothesensammlung: perfekte Sicherheit - Definition	UG	Tafel	10 min
	- Unter welchen Bedingungen erhält man ein perfekt sicheres Verfahren?			
Erarbeitung 2	- Satz von Shannon mit Beweis - One-Time-Pad	PA	PC, Excel File, Arbeitsblatt, Beweispuzzle, Datei „Beweis.pdf“	40 min
Sicherung 2	- Satz von Shannon mit Beweis - One-Time-Pad - Caesar-Verfahren	UG	Overheadprojektor, Folien	20 min

Tabelle 6.2: Tabellarischer Verlaufsplan Einheit 2

[1] Partnerarbeit

Material

Arbeitsblatt 2

Datum:	**Analyse des Caesar-Verfahrens**	Kryptographie AB 2


Partnerarbeit!

A1 Öffnet beide das Programm CrypTool.
Unter „Datei → Neu“ könnt ihr eine Textdatei erstellen. Schreibt eurem Gruppenpartner eine kurze Nachricht (2-3 Zeilen) und verschlüsselt diese unter „Ver-/Entschlüsseln → symmetrisch → Caesar“. Der Wert des ersten Alphabetzeichens soll 1 sein. Gebe ein Alphabetzeichen als Schlüssel ein. Speichert die verschlüsselte Nachricht adressiert an euren Partner im Kursordner mit dem Namen „An ...“ ab.

A2 Öffne die Datei, die an dich adressiert ist.
Unter Analyse → symmetrische Verschlüsselung → Ciphertext Only → Caesar wird das Programm dazu aufgefordert den Text zu entschlüsseln. Es öffnen sich mehrere Fenster.
Welche Analysen macht das Programm, um den Text zu entschlüsseln? Macht euch Notizen zu der Methode, die das Programm anwendet.

? Im File Hilfe.docx findet ihr einen Link zur Erklärung der Analyse durch CrypTool.

Arbeitsblatt 3

Datum:	**Perfekte Sicherheit**	Kryptographie AB 3



Definition: Perfekte Sicherheit
Ein Verschlüsselungsverfahren heißt *perfekt sicher*, wenn die Wahrscheinlichkeit eines Klartextes nicht vom vorliegenden Geheimtext abhängt:

$$P(m|c) = P_M(m)$$

A1 Öffnet die Datei „PerfekteSicherheit.xlsx“.
Euer Ziel: Verändert das Verschlüsselungssystem so, dass ein perfekt sicheres Verfahren entsteht.
Formuliert die Bedingungen unter denen euch dies gelungen ist in der linken Spalte.

Eigene Beobachtungen	Satz von Shannon

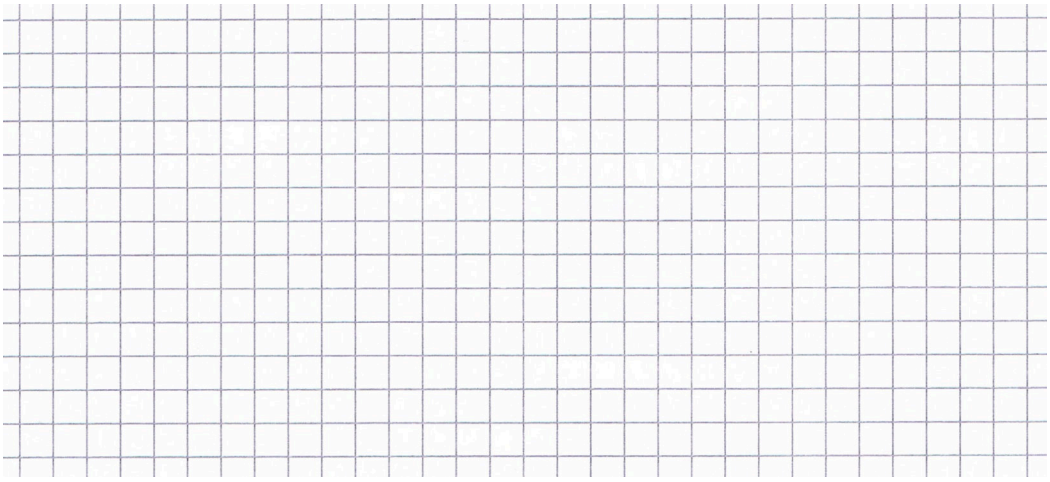
Der Satz von Shannon

A2 Hole dir am Pult einen Umschlag. Du findest darin:

- Den Satz von Shannon: Er beschreibt die Bedingungen unter denen ein Verfahren als perfekt sicher gilt. Klebe ihn in die rechte Spalte von Aufgabe 1. Vergleicht eure Bedingungen mit den Bedingungen des Satzes.
- Ein Beweispuzzle zur Rückrichtung des Satzes: Markiere zunächst im Satz von Shannon in rot die Voraussetzung und in blau die Behauptung. Lege und klebe dann den Beweis. Ergänze Begründungen.

Beweis:

A3 Informiere dich im Internet über das sogenannte „One-Time-Pad“. Begründe, warum das Verfahren perfekt sicher ist.





Zusatzaufgabe!

a) Unter welchen Bedingungen wäre das Caesar-Verfahren perfekt sicher?
b) Die Hinrichtung des Satzes ist etwas schwieriger zu beweisen. Versuche eine Beweisidee zu finden oder den Beweis in der Datei „Beweis.pdf“ nachzuvollziehen.

6.3 Diffie-Hellman-Schlüsselaustausch

Lernziele und Kompetenzen

Grobziel: Die SuS können den Diffie-Hellman Schlüsselaustausch hinsichtlich Durchführung und Sicherheit diskutieren.

Feinziele:

Die SuS können...

- das Schlüsselaustauschproblem als grundlegendes Problem von Verschlüsselungsverfahren nennen.
- Addition, Multiplikation und Potenzierung in Restklassen durchführen.
- das Schlüssel-Schloss Modell mit dem Schlüsselaustauschprotokoll vergleichen.
- das Diffie-Hellman Schlüsselaustauschprotokoll korrekt widergeben.
- den Zusammenhang zwischen der Wahl der Basis g und der Größe des Schlüsselraumes erläutern.
- das Schlüsselaustauschprotokoll auf Angriffsmöglichkeiten hin untersuchen.

Kompetenzen:

Die SuS...

- schulen ihre Kompetenz im mathematischen argumentieren [K1], indem sie die Korrektheit des Schlüsselaustausches, sowie die Abhängigkeit der Sicherheit von der Wahl der Basis g begründen.
- schulen ihre Kompetenzen im Umgang mit formalen Elementen der Mathematik [K5], indem sie das modulare Rechnen erlernen und üben.
- vertiefen ihre Kompetenzen im mathematischen kommunizieren [K6], indem sie einen Vergleich zwischen Schlüssel-Schloss Modell und dem Diffie-Hellman Verfahren anstellen sowie eigene Überlegungen zum Thema Sicherheit darlegen.

Didaktische Analyse

Relevanz des Gegenstandes

Der Diffie-Hellman Schlüsselaustausch ist ein Paradebeispiel für die Public-Key-Kryptographie. Ein großes kryptographisches Problem wird durch die geschickte Anwendung von Mathematik gelöst. Der Algorithmus findet seit seiner Entdeckung viele Anwendungen, u. a. in Virtuellen Privaten Netzwerken.

Struktur des Inhalts

Um ein tiefes Verständnis über den Diffie-Hellman Schlüsselaustausch zu erhalten, sind einige Erkenntnisschritte notwendig. Zunächst muss der Schlüsselaustausch als Schwachstelle der bisher gelernten Systeme kennengelernt werden. Dies soll Inhalt der Einführung sein. In der vorigen Stunde wurde das One-Time-Pad besprochen und als perfekt sicher herausgestellt. Ein „Durchspielen“ der Kommunikation mit dem One-Time-Pad führt zu dem Schlüsselaustauschproblem: Nachdem ein Schüler eine Nachricht verschlüsselt hat, kann er diese an seinen Kommunikationspartner übermitteln - dieser Schritt ist perfekt sicher. Doch dann stellt sich für die SuS das Problem der Entschlüssselung: Der Partner muss an den Schlüssel gelangen. Wird dieser jedoch über den gleichen Kanal wie die verschlüsselte Botschaft versendet, so ist die Sicherheit aufgehoben. Das One-Time-Pad soll hierbei nicht klassisch mit binärer Verschlüsselung genutzt werden, sondern als die perfekt sichere Abwandlung des Caesar-Verfahrens, die letzte Stunde erarbeitet wurde. Dies hat den Vorteil, dass die SuS einfacher eigene Texte damit verschlüsseln können, ohne die Buchstaben vorher binär darstellen zu müssen. Im Anschluss findet die Problemformulierung statt. Die Problemfrage für diese Stunde lautet: „Wie kann ein Schlüssel über einen unsicheren Kanal ausgetauscht werden, ohne dass ein Angreifer den Schlüssel kennt?“ Lösungsansätze zum Problem sollen im Folgenden anhand eines Schlüssel-Schloss Modells erarbeitet werden. Dabei erhalten beide Parteien eine Box, welche jeweils mit zwei Schlössern gesichert ist. Je ein Kommunikationspartner besitzt zu einem der Schlösser den passenden Schlüssel. Durch geeignetes Hin- und Herschicken der nie ganz geöffneten Boxen wird die Schlüsselerzeugung simuliert. Hier wird für die SuS ein Prinzip der Public-Key-Verschlüsselung deutlich: Es werden nur Inhalte übermittelt, mit denen der Kommunikationspartner weiter agieren kann. Dies ist zunächst nicht nur der verschlüsselte Text, sondern auch Sendungen zur Schlüsselproduktion finden statt. Die Vorgehensweise des Modellbeispiels soll in der linken Spalte einer Tabelle festgehalten werden. Im Anschluss soll der Algorithmus kennen gelernt werden. Vorher muss jedoch ein Exkurs zum Thema modulares Rechnen stattfinden. Da die SuS bereits in Kontakt zu der Modulo-Schreibweise gekommen sind, sollte hier lediglich eine Wiederholung stattfinden. Dies soll erneut am Beispiel der Caesar-Chiffre geschehen. Alternativ könnte das Uhrenmodell als Grundlage dienen. Um allerdings thematisch bei der Kryptographie zu bleiben, wurde sich für erstere Möglichkeit entschieden. Dazu soll eine Tabelle nochmals deutlich machen, was passiert, sobald die Summe von Klartextwert und Schlüsselwert größer als 25 ist. Weiter wird die Annahme getätigt, es wären Schlüssel größer 25 zugelassen. Die SuS werden zunächst dazu aufgefordert, Buchstaben mithilfe der Tabelle zu verschlüsseln, eine passende Kongruenzgleichung dazu aufzustellen und eine Begrüngung über Teilbarkeit mit Rest zu liefern. Die Begründung über die Teilbarkeit erleichtert das eigenständige Finden einer rechnerischen Methode zur Verschlüsselung. Eine Regel zur modularen Addition soll eigenständig formuliert werden. Wichtig ist hierfür, dass die SuS den Begriff der „modularen Reduktion“ kennen. Diese Information soll auf dem zugehörigen Arbeitsblatt gegeben werden.

Um den Lernfluss der einzelnen Schüler nicht zu beeinflussen, soll eine erste Sicherung wieder individuell stattfinden können. Dazu eignet es sich, die Ergebnisse zum Abgleich zur Verfügung zu stellen. Im Folgenden soll die Multiplikation und Potenzierung modulo n geübt werden. Da die Rechenregeln hier dem gleichen Prinzip wie bei der Addition folgen, wird auf eine erneute Regelformulierung verzichtet. Stattdessen bekommen die SuS einen Tipp zur Lösung der Aufgaben. Da in dieser Phase mit einer großen Heterogenität des Kurses zu rechnen ist, werden erneut Zusatzaufgaben angeboten. Um das mathematische Niveau zu heben, sollen zwei Aussagen bewiesen werden:

- Es gilt $m \equiv 0 \bmod n$ genau dann, wenn n ein Teiler von m ist.
- Eine Zahl m ist ungerade, genau dann wenn gilt: $m \equiv 1 \bmod 2$.

Nach dieser Phase findet eine weitere Sicherung statt, diesmal gemeinsam im Kurs. Mögliche Unklarheiten können an dieser Stelle besprochen werden.
Es kann nun der Algorithmus an geeigneten Zahlen erprobt werden. Die gemeinsame Wahl der beiden Parteien über die Zahlen p und g kann vom Lehrer vorausgewählt werden. Generell muss hier die Entscheidung getroffen werden, ob die Auswahl von g thematisiert wird. Falls nein, so sollte eine Vorauswahl von g getroffen werden. Dies hätte den Vorteil, dass, wie beim Schlüsselaustauschprotokoll verlangt, g eine Primitivwurzel ist. In dieser Unterrichtsstunde soll jedoch der Zusammenhang zwischen der Wahl von g und der Größe des Schlüsselraumes entdeckt werden. Um den Zugang zur Thematik zu erleichtern, wird also auf eine Vorauswahl von g verzichtet. Die SuS werden aufgefordert eine Zahl zwischen 1 und p zu wählen. Hierbei ist nicht entscheidend, ob die Zahl g eine Primitivwurzel ist, die Schlüsselerzeugung funktioniert trotzdem. Der Unterschied entsteht bei der Größe des resultierenden Schlüsselraumes: Je größer dieser ist, desto schwieriger ist es für einen Angreifer das System zu knacken. Die SuS werden also danach gefragt, wie viele mögliche Schlüssel mit ihrer Wahl generiert werden können. Anschließend sollen, durch Ausprobieren der anderen Möglichkeiten von g, Unterschiede festgestellt werden. Um diese Analyse nicht unnötig komplex werden zu lassen, ist es sinnvoll, wenigstens die Primzahl p vorzugeben. Die Wahl $p = 5$ hat folgende Vorteile: Die Wahrscheinlichkeit eine Primitivwurzel zu wählen, liegt bei 50 %. Um alle möglichen Zahlen für g zu testen, bleiben nur 3 weitere übrig. Die Zahlen 2 und 3 sind Primitivwurzeln, es können mit ihnen 4 verschiedene Schlüssel erzeugt werden. Die Zahlen 1 und 4 erzeugen nur zwei verschiedene Schlüssel. Im Anschluss kann die Zahl g, mit welcher man durch Potenzieren alle Zahlen $1 \ldots (p-1)$ erreichen kann, als Erzeuger betitelt werden. Diese Definition ist didaktisch stark reduziert. Sie bezieht sich nur auf das Beispiel der multiplikativen Einheitengruppe $\mathbb{Z}_p^*$. Es wird hier bewusst der Begriff Erzeuger statt Primitivwurzel eingeführt, da dieser intuitiv besser verstanden werden kann. Zunächst aber soll von den SuS der Vergleich zum Schlüssel-Schloss Modell vollzogen werden. Eine ausgefüllte Tabelle könnte wie folgt aussehen:

Schlüssel-Schloss Modell	Diffie-Hellman Verfahren
Schlüssel befindet sich in Box	unbekannter Schlüssel
pro Partei verschließt ein Schloss die Box	beide Parteien müssen agieren, um einen Schlüssel zu generieren
Parteien öffnen Schlösser	Potenzierung modulo n
bei Übermittlung ist Box immer durch mind. 1 Schloss verschlossen	Rückoperation ist nicht möglich?

Die letzte Zeile der rechten Spalte wird den SuS Schwierigkeiten bereiten bzw. sie zu der Frage bringen, ob die Potenzierung modulo n ausreicht, um Eve den Angriff unmöglich zu machen. Dazu passend wird an dieser Stelle eine Zusatzaufgabe angeboten: Die SuS werden aufgefordert, Angriffsmöglichkeiten auf den Schlüsselaustausch herauszustellen.
Im Anschluss werden die Ergebnisse der Erarbeitungsphase gesichert. Das Protokoll an sich muss nicht extra gesichert werden, da die Vorgehensweise aus Aufgabe 1 hervorgeht. Es wird lediglich, im Zuge der Besprechung von Aufgabe 3, darauf aufmerksam gemacht, dass im Folgenden für die Zahl g immer ein Erzeuger genommen werden soll und dass die Primzahl p natürlich immer neu gewählt wird. Im Anschluss werden die Angriffsmöglichkeiten vorgestellt. Zum einen kann von den SuS die Idee genannt werden, dass ein Angreifer durch Ausrechnen des Logarithmus an die geheimen Zahlen gelangen kann. Dies führt auf das diskrete Logarithmusproblem, welches als zentraler Sicherheitsfaktor herausgestellt wird. Der Lehrer erklärt, dass dieses Problem zwar mit kleinen Zahlen durch Ausprobieren, mit großen Zahlen jedoch praktisch nicht zu lösen ist. Des Weiteren kann der Man-in-the-Middle Angriff genannt werden und somit die Thematik auf Signaturen gelenkt werden. Falls keiner der SuS zu der Zusatzaufgabe gekommen ist, wird die Frage nach den Angriffsmöglichkeiten direkt der ganzen Klasse gestellt. Ziel ist es, das diskrete Logarithmusproblem und den Man-in-the-Middle Angriff gemeinsam mit den SuS zu formulieren.

Methodische Analyse

Der Einstieg erfolgt anhand des One-Time-Pads, das letzte Stunde als perfekt sicheres System vorgestellt wurde. Dazu wird ein Abreißblock mitgebracht, auf welchem Caesar Schlüssel vermerkt sind (siehe Abbildung 6.5). Ein Schüler wird aufgefordert, anhand des Blockes die Funktionsweise zu erklären und die perfekte Sicherheit zu wiederholen. Der Schüler wird dann vom Lehrer direkt in ein Rollenspiel versetzt: Es wird erklärt, dass in der Kryptographie die Charaktere Alice, Bob und Eve, Sender, Empfänger und Angreifer symbolisieren. Der Schüler mit dem Block in der Hand ist nun Alice (oder Bob). Er soll sich einen Kommunikationspartner

wählen und diesem mit dem Block eine kurze Nachricht zukommen lassen. Ausreichend ist hier ein kurzes Wort, um die Verschlüsselung nicht unnötig lang dauern zu lassen. Während der Schüler verschlüsselt, wird innerhalb des Kurses eine Eve gewählt. Diese darf sich zwischen Alice und Bob positionieren und alles, was die beiden sich zukommen lassen, abfangen, lesen und protokollieren. Im Anschluss findet die Übermittlung statt. Der Lehrer zieht sich zurück, um dem Kurs freies Spiel zu lassen. Vermutlich stellt sich recht schnell das Problem, dass zwar der verschlüsselte Text problemlos in Eves Hände gelangen kann, der Abreisblock jedoch nicht auf dem gleichen Weg übermittelt werden kann.



Abbildung 6.5: Abreißblock zur Veranschaulichung des One-Time-Pads, Quelle: Eigene Darstellung

Im Anschluss findet die Problemformulierung statt. Dies geschieht an der Tafel. Die SuS formulieren eine Problemfrage, die vom Lehrer notiert wird. Die Erarbeitungsphase beginnt mit einer weiteren Simulation. Das Schlüssel-Schloss Modell soll in einem weiteren Rollenspiel erarbeitet werden. Alternativ könnte ein Schaubild dazu besprochen werden. Dies würde jedoch nicht das Problemlösevermögen der SuS sowie die Interaktion im Kurs fördern. Der Kurs wird in zwei Hälften geteilt. Eine Seite symbolisiert Alice, die andere Bob. Ein Schüler spielt die Angreiferin Eve. Beide Seiten bekommen jeweils folgende Materialien: Eine verschlossene Box, inder sich zwei identische Abreißblöcke befinden, mit je zwei Schlössern sowie den Schlüssel für das eigene Schloss (siehe Abbildung 6.6).



Abbildung 6.6: Schlüssel-Schloss Modell zur Veranschaulichung des Diffie-Hellman Schlüsselaustausches, Quelle: Eigene Darstellung

Wieder zieht sich der Lehrer zurück. Nachdem die SuS es geschafft haben, die Schlüssel auszutauschen, ohne dass sie Eve zu Gesicht bekommt, wird das erste Arbeitsblatt ausgeteilt (AB 4). Dieses Arbeitsblatt ist zudem auf Folie vorhanden, sodass die linke Seite der Tabelle in Aufgabe 2 gemeinsam im Unterrichtsgespräch ausgefüllt werden kann. Es wird vom Lehrer darauf hingewiesen, dass im weiteren Verlauf der Stunde ein mathematisches Verfahren kennengelernt wird, das es ermöglicht, gemeinsam einen Schlüssel zu generieren. Dazu müssen aber zunächst mathematische Inhalte bereitgestellt werden. Arbeitsblatt 5 wird ausgeteilt und in Einzelarbeit berarbeitet. Die Zwischensicherung findet individuell statt. Dazu liegt ein Vergleichsblatt auf dem Pult bereit. Zur weiteren Sicherung wird eine Folie mit Aufgabe A4 von Arbeitsblatt 5 aufgelegt. Der Lehrer trägt die von den SuS genannten Ergebnisse in die Tabelle ein. Schüler, welche eine Zusatzaufgabe bearbeitet haben, dürfen ihre Beweisführung auf Folie vorführen. Im Anschluss kann auf Arbeitsblatt 4 weitergearbeitet werden. Die Sicherung der Ergebnisse erfolgt wieder mittels Overheadprojektor und Folie. Die Besprechung der Angriffsmöglichkeiten kann wieder durch eine kurze Simulation unterstützt werden. Um Zeit zu sparen, kann die Rolle der Eve vom Lehrer übernommen werden. Anschließend wird das diskrete Logarithmusproblem und der Man-In-The-Middle Angriff an der Tafel formuliert und von den SuS auf das Arbeitsblatt übernommen.

Verlaufsplan

Phase	Inhalt	UV	Medien	Zeit
Einführung	- Wiederholung One-Time-Pad - Simulation der Kommunikation	UG, SG	Abreißblock	7 min
Problemformulierung	Wie kann ein Schlüssel über einen unsicheren Kanal ausgetauscht werden, ohne dass ein Angreifer den Schlüssel kennt?	UG	Tafel	3 min
Erarbeitung 1	Schlüssel-Schloss Modell: Simulation und Sicherung	SG, UG	2 Boxen, 4 Schlösser und passende Schlüssel, Overheadprojektor und AB 4 auf Folie	20 min
Exkurs	Modulares Rechnen	EA[1]	Arbeitsblatt 5, Taschenrechner	20 min
Erarbeitung 2	- Durchführung des Schlüsselaustausches - Einführung des Begriffs „Erzeuger“ - Zusatz: Angriffsmöglichkeiten	PA	Arbeitsblatt 4, Taschenrechner	25 min
Sicherung 2	Besprechung: Aufgabe 2 und 3, Sicherung: diskretes Logarithmusproplem, Man-In-The-Middle Angriff	UG	Folie, Tafel	15 min

Tabelle 6.3: Tabellarischer Verlaufsplan Einheit 3

[1] Einzelarbeit

Material

Arbeitsblatt 4

Datum:	**Diffie-Hellman Schlüsselaustausch**	Kryptographie AB 4


Partnerarbeit!

A1 Einigt euch, wer von euch Alice und wer Bob ist! Führt die Anweisungen in der Tabelle aus.

	Alice	Bob
Wählt gemeinsam:	Es ist $p = 5$ eine Zahl $g \in \{1, \ldots, p-1\}$ $g =$	
Wähle geheim:	$a \in \{2, \ldots, p-1\}$ $a =$	$b \in \{2, \ldots, p-1\}$ $b =$
Berechne und sende:	$A = g^a \bmod p =$	$B = g^b \bmod p =$
Empfange:	$B =$	$A =$
Berechne:	$k = B^a =$	$k = A^b =$

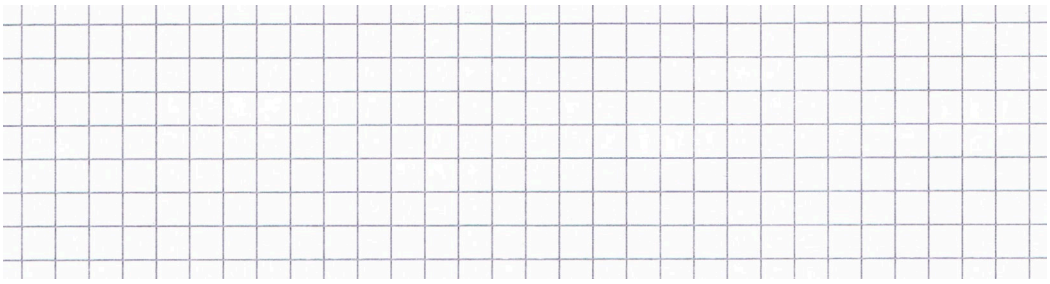
Begründet: Alice und Bob erhalten den gleichen Schlüssel k.

A2 Füllt die Tabelle zum Vergleich zwischen dem Schlüssel-Schloss Modell und dem oben durchgeführten Verfahren aus.

Modell	Verfahren

A3 Untersucht anhand folgender Fragen den Zusammenhang zwischen g und dem Schlüsselraum:

- Wie viele mögliche Schlüssel können mit eurer Wahl von g erreicht werden?
- Ist die Schlüsselmenge von der Wahl von g abhängig?
- Begründet, warum eine geeignete Wahl von g für die Sicherheit des Schlüsselaustausches wichtig ist.



Definition: Die Zahl g, mit welcher durch Potenzierung mod p alle Zahlen $1, \ldots, (p-1)$ erreicht werden können, heißt *Erzeuger*.



Die Angreiferin Eve möchte die Kommunikation zwischen Alice und Bob beeinflussen. Welche Möglichkeiten hat sie trotz des oben vorgstellten Verfahrens?

Arbeitsblatt 5

Datum:	**Modulares Rechnen**	Kryptographie AB 5

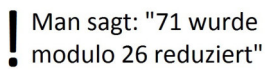

Einzelarbeit!

A1 Die folgende Tabelle hilft bei der rechnerischen Umsetzung des Caesar Verfahrens. Lese dir zur Wiederholung die mathematische Darstellung des Verfahrens durch!

A	B	C	D	E	F	...	X	Y	Z
0	1	2	3	4	5		23	24	25
26									

Verschlüssele wie angegeben und stelle die zugehörigen Kongruenzgleichungen auf:

Verschlüsselung	Kongruenzgleichung	Begründung
$m = Z, k = 3$ $\Rightarrow c = C$	$28 \equiv 2 \mod 26$	denn $28 : 26 = 1$ Rest **2**
$m = Y, k = 25$ $\Rightarrow c =$		
$m = A, k = 5$ $\Rightarrow c =$		
Angenommen, es wären Schlüssel $k > 25$ erlaubt:		
$m = F, k = 26$ $\Rightarrow c =$		
$m = Z, k = 56$ $\Rightarrow c =$		
$m = B, k = 70$ $\Rightarrow c =$		



Erkennst du eine Methode, wie du ohne die Hilfe der Tabelle verschlüsseln kannst? Verschlüssele das Wort „MODULO“ mit dem Schlüssel $k = 56$.

A2 Formuliere eine Regel zur Modularen Addition!

A3 Vergleiche deine bisherigen Ergebnisse mit dem Lösungsblatt auf dem Pult!

A4 Führe folgende Berechnungen durch:

! Multiplikation und Potenzierung modulo n erfolgen nach dem gleichen Prinzip wie die Addition

Addition	Multiplikation	Potenzierung
$4 + 5 \equiv __ \bmod 4$	$3 \cdot 10 \equiv __ \bmod 10$	$3^3 \equiv __ \bmod 4$
$2 + 3 \equiv __ \bmod 5$	$4 \cdot 5 \equiv __ \bmod 3$	$2^4 \equiv __ \bmod 5$



Zusatzaufgabe!

Begründe:

i) Es gilt $m \equiv 0 \bmod n$ genau dann, wenn n ein Teiler von m ist.

ii) Eine Zahl m ist ungerade, genau dann, wenn gilt: $m \equiv 1 \bmod 2$.

7 Fazit

> „*Cryptography is a charming and rewarding way to introduce into the classroom subjects of traditional mathematics, algebra, modular arithmetic, computational linguistic, combinatorics, algorithms,...*“[15], S.2

Massimo Borelli beschreibt in diesem Zitat die Potentiale, die eine Einbindung der Kryptographie in den Unterricht mit sich bringen kann. In dieser Arbeit wurde eine Unterrichtsreihe beschrieben, welche einige dieser Potentiale nutzt, um Schülern erste Inhalte eines mathematischen Studiums aufzuzeigen. Es wurden dazu zunächst theoretische Grundlagen erläutert, um im Anschluss näher auf die Unterrichtsinhalte eingehen zu können. Nach der Darlegung von kryptographischen Grundkonzepten wurden historische Verfahren, wie die Skytala von Sparta, das Caesar-Verfahren und das Vigenère-Verfahren, sowie asymmetrische Verfahren wie der RSA-Algorithmus und der Diffie-Hellman Schlüsselaustausch beschrieben. Für die Unterrichtsreihe wurden, aus der Fülle der möglichen Themen, die drei Schwerpunkte „Verschlüsselungsverfahren“, „perfekte Sicherheit“ und „Diffie-Hellman Schlüsselaustausch“ gewählt. Bei der Konzeption wurde besonderen Wert auf einen motivierenden Unterricht gelegt, welcher erste Studieninhalte vermittelt. Dabei wurden die unterschiedlichen Lernvoraussetzungen der Schüler und Schülerinnen berücksichtigt.
In weiteren Überlegungen kann ein Ausbau der Reihe stattfinden, um noch mehr Inhalte, sowohl im Bereich der Kryptographie, als auch zur Studiumsvorbereitung, zu vermitteln. Thematisch eignet sich hierfür in besonderem Maße das RSA-Verfahren. Je nach Zusammensetzung des Kurses kann der Fokus stärker auf mathematische Inhalte oder anschauliche Beispiele gelegt werden. Die Inhalte und Unterrichtsideen eignen sich zudem zur Umsetzung einer Projektwoche, welche auf diesen Überlegungen aufbauend konzipiert werden könnte.

Literaturverzeichnis

[1] Franziska Badenschier. Kryptografieren leicht gemacht – Schreiben Sie in Geheimschrift. planet-wissen.de, Zugriff November 2013.

[2] Klaus Becker. Informatik in der Schule - Station: Chiffrierung mit dem Vigenère-Verfahren. inf-schule.de, Zugriff Januar 2014.

[3] Albrecht Beutelspacher. *Kryptologie*. Vieweg Friedr. + Sohn Ver, 2007.

[4] Albrecht Beutelspacher, Jörg Schwenk, and Klaus-Dieter Wolfenstetter. *Moderne Verfahren der Kryptographie: Von RSA zu Zero-Knowledge (German Edition)*. Vieweg + Teubner Verlag, 2010.

[5] Detlef Borchers. Assange: Kryptografie ist die ultimative Form des gewaltlosen Widerstandes. Heise Online, zitiert November 2013.

[6] Thomas Borys. *Codierung und Kryptologie*. Vieweg+Teubner Research, 2011.

[7] Johannes Buchmann. *Einführung in die Kryptographie, 5. Aufl.* Springer, 2010.

[8] Wolfgang Ertel. *Angewandte Kryptographie*. Hanser Fachbuchverlag, 2003.

[9] Prof. Bernhard Esslinger. Häufigkeitsanalyse. CrypTool Online, Zugriff Februar 2014.

[10] Andreas Gathmann. Algebraische Strukturen; Vorlesungsskript Universität Kaiserslautern 2010.

[11] Christian Karpfinger and Hubert Kiechle. *Kryptologie -Algebraische Methoden und Algorithmen, 1. Aufl.* Vieweg+Teubner, 2010.

[12] Kulturministerkonferenz. Bildungsstandards im Fach Mathematik für die Allgemeine Hochschulreife, 2012.

[13] Thomas Markwig. Algebraische Strukturen; Vorlesungsskript Universität Kaiserslautern Oktober 2008.

[14] Thomas Markwig. Elementare Zahlentheorie; Vorlesungsskript Universität Kaiserslautern März 2010.

[15] Andrea Sgarro Massimo Borelli, Anna Fioretto and Luciana Zuccheri. Cryptography and statistics: A didactical project.

[16] Wissenschaft und Weiterbildung Rheinland-Pfalz Ministerium für Bildung. Lehrplan Informatik Grund- und Leistungsfach Einführungsphase und Qualifikationsphase der gymnasialen Oberstufe.

[17] Wissenschaft und Weiterbildung Rheinland-Pfalz Ministerium für Bildung. Lehrplan Mathematik Grund- und Leistungsfach Jahrgangsstufen 11 bis 13 der gymnasialen Oberstufe,1998.

[18] Peter Mörters and Heinrich v. Weizäcker. Stochastische Methoden; Vorlesungsskript Universität Kaiserslautern WS 2009/10.

[19] Heise Online. NSA Skandal: Was bisher geschah. Heise Online, Zugriff Januar 2014.

[20] Jörg Rothe. *Komplexitätstheorie und Kryptologie.* Springer-Verlag Berlin Heidelberg, 2008.

[21] Simon Singh. *The Code Book, 5. Aufl.* Delacorte Press, 2001.

[22] Manfred Baum u.a. *LS Stochastik, 1. Aufl.* Ernst Klett Verlag, 2003.

[23] Dr. Jörg Vogel. Kryptologie – von einer Geheimwissenschaft zu einer Wissenschaft von den Geheimnissen; Vorlesungsskript Universität Jena WS 2006/07.

Anhang

A) Mathematische Grundlagen

Dieser Abschnitt dient als Nachschlagewerk zu den verwendeten mathematischen Grundlagen. Die Beweise zu den Sätzen sind jeweils in der angegebenen Literatur nachzulesen.

A1 Stochastik [18]

Definition: Messbarer Raum

Das Tupel $(\Omega, \mathcal{A})$ heißt *messbarer Raum*, wenn gilt:

- Ω ist eine nichtleere Menge
- $\mathcal{A} \subseteq \mathcal{P}(\Omega)$ ist eine σ- Algebra auf Ω, d.h.:
  1. $\Omega \in \mathcal{A}$
  2. Falls $A \in \mathcal{A}$ dann gilt dies auch für das Komplement: $A^C \in \mathcal{A}$
  3. Falls $A_1, A_2, A_3, \ldots \in \mathcal{A}$ dann ist auch $\bigcup_{i=1}^{\infty} A_i \in \mathcal{A}$

Die Elemente aus Ω heißen Ergebnisse, die Elemente aus $\mathcal{A}$ heißen Ereignisse.

Definition: Wahrscheinlichkeitsverteilung

Man nennt $P : \mathcal{A} \to [0, 1]$ *Wahrscheinlichkeitsverteilung* auf $(\Omega, \mathcal{A})$, falls gilt:

- $P(\Omega) = 1$
- für $A_1, A_2, A_3, \ldots$ mit $A_i \cap A_j \neq \emptyset, i \neq j$ gilt $P(\bigcup_{i=1}^{\infty} A_i) = \sum P(A_i)$

$(\Omega, \mathcal{A}, P)$ heißt *Wahrscheinlichkeitsraum*.

Definition: Bedingte Wahrscheinlichkeit/ Stochastische Unabhängigkeit

Sei $(\Omega, \mathcal{A}, P)$ ein Wahrscheinlichkeitsraum, $B \in \mathcal{A}$ ein Ereignis mit $P(B) > 0$. Für $A \in \mathcal{A}$ sei die *bedingte Wahrscheinlichkeit* $P(A|B)$ gegeben durch:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Die Ereignisse A und B heißen *stochastisch unabhängig* wenn gilt:

$$P(A \cap B) = P(A) \cdot P(B)$$

Satz von Bayes:

Für A, $B \in \mathcal{A}$ mit $P(A) > 0$ und $P(B) > 0$ gilt:

$$P(A) \cdot P(B|A) = P(B) \cdot P(A|B)$$

A2 Zahlentheorie

Der erweiterte euklidische Algorithmus [10], S.69

Sei R ein euklidischer Ring mit euklidischer Funktion $\delta : R\{0\} \to \mathbb{N}$ und $a_0, a_1 \in \mathbb{R}$. Für $n \geq 2$ definiere, solange $a_{n-1} \neq 0$, eine rekursive Folge $a_0, a_1, a_2, \ldots, a_N \in \mathbb{R}$ wie folgt:

$$a_{n-2} = q_n a_{n-1} + r_n$$

für gewisse $q_n, r_n \in \mathbb{R}$. Setze $a_n := r_n$.
Für die Folge gilt:

a) Das Verfahren bricht nach endlich vielen Schritten ab, dh. $a_N = 0$ für ein $N \in \mathbb{N}$.

b) $a_{N-1} \in ggT(a_0, a_1)$

c) Für alle $n = 0, \ldots, N-1$ lässt sich a_{N-1} schreiben als:

$$a_{N-1} = d_n a_n + e_n a_{n+1}$$

für gewisse $d_n, e_n \in \mathbb{R}$. Insbesondere ist $a_{N-1} \in ggt(a_0, a_1)$ eine Linearkombination von a_0 und a_1.

***„Square and Multiply"*-Algorithmus** [20], S.352

Zur Berechnung von

$$b^a \bmod n$$

nutzt der Algorithmus folgende Schritte:

1. Berechnung der Binärentwicklung von a:

$$a = \sum_{i=0}^{k} a_i 2^i$$

2. Sukzessive Berechnung von b^{2^0}, b^{2^1},..., b^{2^k} durch Anwendung von

$$b^{2^{i+1}} \equiv (b^{2^i})^2 \bmod n$$

3. Berechnung von:

$$b^a = \prod_{i=0, a_i=1}^{k} b^{2^i} \bmod n$$

Die g-adische Darstellung [7], S.3

Sei $g \in \mathbb{N}$, $g > 1$. Für alle $a \in \mathbb{N}$ existiert ein eindeutiges $k \in \mathbb{N}$ und eine eindeutig bestimmte Folge $(a_1, \ldots, a_k) \in \{0, \ldots, g-1\}^k$ mit $a_1 \neq 0$ und

$$a = \sum_{i=1}^{k} a_i g^{k-i}$$

Es ist $k = \lfloor \log_g a \rfloor + 1$ und $a_i \in \mathbb{Z}$ ist der Quotient von $a - \sum_{j=1}^{i-1} a_j g^{k-j}$ und g^{k-i}, $1 \leq i \leq k$.

Der Kleine Satz von Fermat [14], S.42

Sei $p \in \mathbb{P}$ eine Primzahl. Dann gilt für alle $a \in \mathbb{Z}_n$:

$$a^p \equiv a \bmod p$$

Der Chinesische Restsatz [13], S.134

Seien $n_1, \ldots, n_r \in \mathbb{Z} \setminus \{0\}$ paarweise teilerfremd und $N = n_1 \cdots n_r$, $N_i = \frac{N}{n_i}$.

a) Zu beliebigen $a_1, \ldots, a_r \in \mathbb{Z}$ existiert eine Lösung $x \in \mathbb{Z}$ des Kongruenzgleichungssystems:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

b) Sei $\bar{x_i} = \bar{N_i}^{-1} \in \mathbb{Z}_{n_i}$ für $i = 1, \ldots, r$. Dann ist

$$x' = \sum_{i=1}^{r} N_i \cdot x_i \cdot a_i \in \mathbb{Z}$$

eine Lösung des Kongruenzgleichungssystems.

c) Die Lösung des Kongruenzgleichungssystems ist modulo N eindeutig bestimmt.

B) Klartext des Beispiels zur Vigenère-Verschlüsselung

"The Vision of Sin"von Alfred Tennyson

Sit thee down, and have no shame,
Cheek by jowl, and knee by knee:
What care I for any name?
What for order or degree?

Let me screw thee up a peg:
Let me loose thy tongue with wine:
Callest thou that thing a leg?
Which is thinnest? thine or mine?

Thou shalt not be saved by works:
Thou hast been a sinner too:
Ruined trunks on withered forks,
Empty scarecrows, I and you!

Fill the cup, and fill the can:
Have a rouse before the morn:
Every moment dies a man,
Every moment one is born.

C) Unterrichtsmaterial

Eine Sammlung des Unterrichtsmaterials zur Nutzung am Computer befindet sich auf beigelegter CD.

Eidesstattliche Erklärung

Name:
Vorname:
Mtk.-Nr.:
Geb.-Datum:
Geb.-Ort:
Studiengang:

Hiermit versichere ich, dass ich die beiliegende schriftliche Arbeit ohne fremde Hilfe erstellt habe. Bei der Erstellung der vorliegenden Arbeit wurden keine weiteren als die angegebenen Quellen und Hilfsmittel benutzt.
Mir ist bewusst, dass bei einem Verstoß gegen obige Erklärung nicht nur die betreffende Prüfungsleistung mit der Note 5,0 wegen Täuschungsversuchs gewertet werden, sondern auch eine Exmatrikulation erfolgen kann.

Ort, Datum, Unterschrift