Einführung in die Kryptologie und ihre Vermittlung im Schulunterricht

Diplomarbeit

in der Studienrichtung

Lehramtsstudium Mathematik - Informatik und Informatikmanagement

zur Erlangung des akademischen Grades Magistra der Naturwissenschaften

eingereicht an der

Fakultät für Mathematik, Informatik und Physik der Universität Innsbruck

von

Aygül Koc

Betreuer der Diplomarbeit

Univ.-Prof. Dipl.-Math. Dr. Tim Netzer
Institut für Mathematik

Innsbruck, 8. August 2019

Inhaltsverzeichnis

Vorwort

Durch die Verbreitung der elektronischen Datenverarbeitung begegnet uns die Verschlüsselung, wenn auch unbewusst, im alltäglichen Leben. Jeder Mensch benutzt heutzutage sein Handy, um eine Nachricht zu versenden, seinen Computer, um eine E-Mail zu schreiben sowie einen Bankomaten, um Geld zu beheben. Nur den wenigsten dürfte allerdings bewusst sein, dass diesen alltäglichen Handlungen das mathematische Teilgebiet Kryptologie zugrunde liegt.

In dieser Arbeit werde ich genauer auf dieses Thema zu sprechen kommen. Wesentliche Begriffe, Grundlagen und Verfahren zur Kryptologie sollen besprochen werden.

Im ersten Abschnitt wird eine mathematische Grundlage aufbereitet, die für die später erklärten Verfahren notwendig ist.

Im zweiten Abschnitt werden, historisch geordnet und motiviert, einige ausgewählte Verschlüsselungsverfahren thematisiert, wobei immer auch die Sicherheit und ein mögliches Knacken der Verschlüsselung im Vordergrund steht. In diesem Bereich beziehe ich mich im Wesentlichen auf Singh (2002), Beutelspacher (2009) und Gómez (2016).

Schließlich ist im dritten Abschnitt eine mögliche Umsetzung einer Unterrichtssequenz zu diesem Thema zu finden. Aus Gründen der täglichen Wichtigkeit der Kryptologie ist es mir ein Anliegen, auch den Schülern einige Details zu diesem Thema in meinem Unterricht nahezulegen.

Es soll noch erwähnt werden, dass ich aus Gründen der Leserlichkeit auf Gendern verzichtet habe. Ich betone aber, dass sehr wohl beide Geschlechter gleichermaßen angesprochen sein sollen.

Zu guter Letzt möchte ich allen danken, die mich bei dieser Arbeit und meinem Studium unterstützt haben. Dazu zählen in erster Linie meine Eltern, die es mir finanziell ermöglicht haben, nochmals einen anderen Bildungsweg einzuschlagen. Außerdem möchte ich mich besonders bei Prof. Dr. Tim Netzer für die Betreuung meiner Arbeit bedanken.

Qxq züqvfkh lfk ghp Ohvhu jdqc ylho Yhujqüjhq ehlp Ohvhq phlqhu Duehlw!

Oder unverschlüsselt: Nun wünsche ich dem Leser ganz viel Vergnügen beim Lesen meiner Arbeit!

1 Mathematische Grundlagen

1.1 Permutation und Kombinatorik

Definition (Permutation)**.** Sei M eine endliche Menge. Eine *Permutation* ist eine bijektive Abbildung von M nach M. Eine Permutation $\pi : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ kann auch als eine $2 \times n$-Matrix angeschrieben werden:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}$$

Beispiel. Gegeben sei die Permutation $\pi : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ mit

$$\pi(1) = 2,\ \pi(2) = 4,\ \pi(3) = 1,\ \pi(4) = 3 \text{ und } \pi(5) = 5 \quad .$$

Wir erhalten folgende 2×5-Matrix:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$$

Satz 1. Die Anzahl der Permutationen einer n-elementigen Menge ist n!

Beweis. Sei o.E.d.A. $M = \{1, 2, \ldots, n\}$.
Für das Bild des ersten Elements 1 gibt es n Möglichkeiten. Für das Bild von 2 stehen noch $n - 1$ Möglichkeiten zur Verfügung, alle außer dem Bild $\pi(1)$ des ersten Elements. Für das Bild von 3 gibt es nur noch $n - 2$ Möglichkeiten, das sind alle bis auf die Bilder $\pi(1)$ und $\pi(2)$, usw. Für das Bild des letzten Elements gibt es nur noch eine Möglichkeit. Also gibt es insgesamt genau $n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 2 \cdot 1 = n!$ Möglichkeiten für die Auswahl einer beliebigen Permutation π von M. □

Definition (Binomialkoeffizient)**.** Es seien $k, n \in \mathbb{N}$ mit $0 \leq k \leq n$. Dann heißt die Zahl

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}$$

Binomialkoeffizient n über k. Dabei ist $0! := 1$.

Mit dem Binomialkoeffizienten kann berechnet werden, wie viele Möglichkeiten es gibt, k Elemente aus einer Menge mit n Elementen auszuwählen, wobei Elemente nicht wiederholt ausgewählt werden und die Reihenfolge der ausgewählten Elemente nicht berücksichtigt wird.

Beispiel (Lotto)**.** Von 45 Kugeln werden genau 6 Kugeln gezogen. Für die erste Kugel gibt es 45 mögliche Kugeln, aus denen gezogen werden kann. Für die zweite Kugel nur noch 44 Möglichkeiten usw. Wenn man 6 Kugeln zieht, ergeben sich dann insgesamt $45 \cdot 44 \cdot 43 \cdot 42 \cdot 41 \cdot 40 \approx 5,9 \cdot 10^9$ mögliche Zahlenkombinationen. Die Reihenfolge der Zahlen spielt aber keine Rolle. Da man 6 Zahlen auf 6! verschiedene Arten anordnen kann[1], ist die berechnete Anzahl der Möglichkeiten um den Faktor 6! zu groß, also muss durch diese Zahl dividiert werden. Somit gibt es

$$\frac{45 \cdot 44 \cdot 43 \cdot 42 \cdot 41 \cdot 40}{6!} = 8.145.060$$

Möglichkeiten, 6 Kugeln aus 45 Kugeln zu ziehen. Wird Zähler und Nenner um 39! erweitert und umgeformt ergibt sich der Binomialkoeffizient:

$$\frac{45!}{39! \cdot 6!} = \frac{45!}{(45-6)! \cdot 6!} = \binom{45}{6}$$

Der Name *Binomialkoeffizient* wird deshalb verwendet, weil mit dieser Formel die Koeffizienten der Binome $(a+b)^n$ berechnet werden. Der binomische Lehrsatz lautet wie folgt:[2]

Satz 2 (Binomischer Lehrsatz)**.** Es seien a, b Elemente eines kommutativen Ringes[3]

[1] Vgl. Satz 1
[2] Für den Beweis dieses Satzes wird auf Rempe und Waldecker (2009), S. 9 verwiesen.
[3] Vgl. Abschnitt 1.5, Definition Ring

(zum Beispiel ganze Zahlen) und n eine natürliche Zahl, dann ist

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

1.2 Euklidischer Algorithmus

Definition (Teiler)**.** Es seien a, $b \in \mathbb{Z}$. Dann heißt a *Teiler* von b (oder a *teilt* b), wenn ein $c \in \mathbb{Z}$ mit $ac = b$ existiert. Schreibweise: $a \mid b$. Ist a kein Teiler von b, schreibt man $a \nmid b$.

Satz 3 (Teilbarkeit von Summe und Differenz)**.** Es seien a, b, $c \in \mathbb{Z}$ mit $a \mid b$ und $a \mid c$. Dann gilt $a \mid (b+c)$ und $a \mid (b-c)$.
In Worten: Wenn a zwei ganze Zahlen teilt, dann teilt a auch deren Summe und Differenz.

Beweis. Aus $a \mid b \Rightarrow \exists x \in \mathbb{Z} : ax = b$ und aus $a \mid c \Rightarrow \exists y \in \mathbb{Z} : ay = c$. Indem wir beide Gleichungen addieren bzw. subtrahieren erhalten wir

$$b + c = ax + ay = a(x+y)$$

bzw.

$$b - c = ax - ay = a(x-y).$$

Da $(x+y)$ und $(x-y)$ ganze Zahlen sind, ist a nach Definition ein Teiler von $(b+c)$ und $(b-c)$. □

Definition (Größter gemeinsamer Teiler)**.** Es seien a, $b \in \mathbb{Z}$ mit $a \neq 0$ und $b \neq 0$. Der größte gemeinsame Teiler von a und b ist die größte Zahl $d \in \mathbb{N}$ mit $d \mid a$ und $d \mid b$. Schreibweise: $d = ggT(a,b)$. Wir nennen a und b *teilerfremd* oder *relativ prim*, wenn $ggT(a,b) = 1$ gilt.

Satz 4 (Division mit Rest)**.** Es seien a, $b \in \mathbb{Z}$ mit $b \neq 0$, so gibt es eindeutig bestimmte Zahlen q, $r \in \mathbb{Z}$ mit $0 \leq r < |b|$, so dass $a = qb + r$ gilt.

Beweis (Eindeutigkeit[4]*).* Es seien $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ mit

[4] Für den vollständigen Beweis inkl. Existenz der Zahlen q und r wird auf Beutelspacher und Zschiegner (2011), S. 65 ff. verwiesen.

$$a = q_1 b + r_1 \text{ und } 0 \leq r_1 < |b|, \text{ sowie } a = q_2 b + r_2 \text{ und } 0 \leq r_2 < |b|.$$

Zu zeigen ist $q_1 = q_2$ und $r_1 = r_2$.

$$\begin{aligned} a = q_1 b + r_1 &= q_2 b + r_2 = a \\ \Leftrightarrow (q_1 - q_2) b &= \underbrace{r_2 - r_1}_{|r_2 - r_1| < |b|} \end{aligned}$$

Dies kann nur für $(q_1 - q_2) = 0$, also $q_1 = q_2$ erreicht werden. Aus $(q_1 - q_2) = 0$ folgt $r_2 - r_1 = 0$, also $r_2 = r_1$. □

Satz 5 (Euklidischer Algorithmus)**.** Es seien a, $b \in \mathbb{N}$. Mit dem Euklidischen Algorithmus kann der größte gemeinsame Teiler von a und b wie folgt berechnet werden:

- Solange a und b nicht gleich sind, ersetzte die größere Zahl durch die Differenz der größeren und der kleineren Zahl.
- Wenn $a = b$ ist, dann ist diese Zahl der größte gemeinsame Teiler von a und b.

Beweis. Aus Satz 3 folgt, dass jede Zahl, die zwei Zahlen teilt, auch deren Differenz teilt. Nun wird die Zahl a bzw. b immer durch die Differenz von a und b ersetzt, wobei die Differenz kleiner ist als a bzw. b. Es ergibt sich also eine kleiner werdende Folge von Zahlen, die aufhört, wenn beide Zahlen gleich sind (dann ist die Differenz der Zahlen Null). Diese verbleibende Zahl ist nach Satz 3 ein gemeinsamer Teiler beider Zahlen. Weil sich der größte gemeinsame Teiler in keinem Schritt des Algorithmus ändert, muss dieser gemeinsame Teiler der größte sein. □

Bemerkung. Der Euklidische Algorithmus kann auch auf Zahlen a, $b \in \mathbb{Z}$ angewandt werden, wobei zuvor a durch $|a|$ und b durch $|b|$ ersetzt wird.

Beispiel. $ggT(299, 161) = ggT(138, 161) = ggT(138, 23) = ggT(115, 23) = ggT(92, 23) = ggT(69, 23) = ggT(46, 23) = ggT(23, 23) = 23$

Wird das mehrfache Subtrahieren der gleichen Zahl durch die Division mit Rest ersetzt, kann das Verfahren beschleunigt werden. In vielen Büchern wird diese Variante aufgrund der schnelleren Durchführbarkeit bevorzugt. Die Division mit Rest liefert somit folgende Form des Euklidischen Algorithmus:

Satz 6 (Euklidischer Algorithmus mit Division mit Rest)**.** Es seien $a, b \in \mathbb{N}$. Wir nehmen im Folgenden an, dass $a > b$ ist, falls $a < b$ können wir die Zahlen vertauschen.

- Berechne Zahlen q und r mit $a = qb + r$ und $0 \leq r < b$.
- Solange $r \neq 0$ ist, setze $a := b$ und $b := r$ und führe den Schritt zuvor aus.
- Wenn $r = 0$ ist, dann ist b der größte gemeinsame Teiler von a und b.

Beispiel. Wir berechnen den $ggT(299, 161)$ vom Beispiel zuvor:

$$\begin{aligned} 299 &= 1 \cdot 161 + 138 & ggT(299, 161) &= ggT(138, 161) \\ 161 &= 1 \cdot 138 + 23 & ggT(161, 138) &= ggT(23, 138) \\ 138 &= 6 \cdot 23 + 0 & ggT(138, 23) &= ggT(0, 23) = 23 \end{aligned}$$

1.3 Erweiterter Euklidischer Algorithmus

Satz 7 (Lemma von Bézout)**.** Es seien $a, b \in \mathbb{Z}$ mit $a \neq 0$ und $b \neq 0$. Dann gibt es Zahlen s und $t \in \mathbb{Z}$ mit

$$sa + tb = ggT(a, b).$$

Man nennt $sa + tb$ eine *Vielfachsummendarstellung* von $ggT(a, b)$. *Insbesondere gilt:* Wenn a und b teilerfremd sind, gibt es Zahlen s und $t \in \mathbb{Z}$ mit $sa + tb = 1$.

Die Zahlen s und t im Lemma von Bézout können mit dem erweiterten Euklidischen Algorithmus berechnet werden.

Satz 8 (Erweiterter Euklidischer Algorithmus)**.** Es seien $a, b \in \mathbb{N}$ mit $a < b$.

- Berechne mit Hilfe des Euklidischen Algorithmus den $ggT(a, b)$:

$$\begin{aligned} a &= q_1 \cdot b + r_1 \\ b &= q_2 \cdot r_1 + r_2 \\ r_1 &= q_3 \cdot r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_{m-2} \cdot r_{n-1} + r_n \\ r_{n-1} &= q_{m-1} \cdot r_n + r_{n+1} \\ r_n &= q_m \cdot r_{n+1} + 0 \end{aligned}$$

  Also ist $ggT(a, b) = r_{n+1}$.

- Beginne bei der vorletzten Gleichung und stelle den letzten Rest als Differenz der Summe und des anderen Summanden dar:

$$r_{n+1} = r_{n-1} - q_{m-1} \cdot r_n$$

- Nun ersetzte in dieser Gleichung r_n durch die Differenz der Summe und des anderen Summanden in der Gleichung zuvor:

$$r_{n+1} = r_{n-1} - q_{m-1} \cdot (r_{n-2} - q_{m-2} \cdot r_{n-1})$$

  An dieser Stelle können die Klammern aufgelöst und nach den Resten zusammengefasst werden. Achtung: Die rechte Seite darf aber nicht vollständig ausmultipliziert werden, dies ergibt nur $1 = 1$.

- Wiederhole bis zur ersten Gleichung den Schritt zuvor.

- Zum Schluss erhalten wir durch das Umordnen der Klammern die gesuchten Zahlen:

$$r_{n+1} = s \cdot a + t \cdot b$$

Beispiel. Sei $a = 101$ und $b = 35$. Wir suchen Zahlen s und t mit $s \cdot 101 + t \cdot 35 = ggT(101, 35)$.

$$
\begin{array}{lcl}
101 = 2 \cdot 35 + 31 & & 1 = 8 \cdot 35 - 9 \cdot (101 - 2 \cdot 35) = 26 \cdot 35 - 9 \cdot 101 \\
35 = 1 \cdot 31 + 4 & & 1 = 8 \cdot (35 - 1 \cdot 31) - 1 \cdot 31 = 8 \cdot 35 - 9 \cdot 31 \uparrow \\
31 = 7 \cdot 4 + 3 & & 1 = 4 - 1 \cdot (31 - 7 \cdot 4) = 8 \cdot 4 - 1 \cdot 31 \uparrow \\
4 = 1 \cdot 3 + 1 & \rightarrow & 1 = 4 - 1 \cdot 3 \uparrow \\
3 = 3 \cdot 1 + 0 & &
\end{array}
$$

Die gesuchten Zahlen sind $s = -9$ und $t = 26$. Der $ggT(101, 35) = 1$.

Mit dem folgenden Schema können wir dieses Verfahren kürzer anschreiben:

101	35	
1	0	101
0	1	35
1	-2	31
-1	3	4
8	-23	3
-9	26	1
35	-101	0

101	35	
1	0	101
0	1	35
$1 - 2 \cdot 0 = 1$	$0 - 2 \cdot 1 = -2$	$101 - 2 \cdot 35 = 31$
$0 - 1 \cdot 1 = -1$	$-2 - 1 \cdot (-1) = 3$	$35 - 1 \cdot 31 = 4$
$1 - 7 \cdot (-1) = 8$	$-2 - 7 \cdot 3 = -23$	$31 - 7 \cdot 4 = 3$
$-1 - 1 \cdot 8 = -9$	$3 - 1 \cdot (-23) = 26$	$4 - 1 \cdot 3 = 1$
$8 - 3 \cdot (-9) = 35$	$-23 - 3 \cdot 26 = -101$	$3 - 3 \cdot 1 = 0$

In der letzten Spalte wird der Euklidische Algorithmus angewandt. Parallel dazu werden die gleichen Operationen auf die anderen zwei Spalten übertragen.

1.4 Primzahlen

Definition (Primzahl)**.** Eine natürliche Zahl $p > 1$ heißt *Primzahl*, wenn die einzigen natürlichen Zahlen, die p teilen, die Zahlen 1 und p sind. Also ist eine natürliche Zahl, die größer als 1 ist, genau dann eine Primzahl, wenn sie nur 1 und sich selbst als Teiler hat.

Satz 9 (Lemma von Euklid)**.** Seien a, $b \in \mathbb{N}$ und sei p eine Primzahl. Dann gilt:

$$p \mid ab \Rightarrow p \mid a \text{ oder } p \mid b.$$

In Worten: Wenn eine Primzahl ein Produkt von Zahlen teilt, dann teilt sie mindestens einen Faktor.

Beweis. Aus $p \mid ab \Rightarrow \exists c \in \mathbb{Z} : cp = ab$. Wir nehmen an, dass p die Zahl a nicht teilt und zeigen, dass p dann den zweiten Faktor b teilt.
Da $p \nmid a$, gilt $ggT(p, a) = 1$. Nach Satz 7 (Lemma von Bézout) gibt es dann ganze Zahlen u und v mit $1 = ua + vp$. Wenn wir diese Gleichung mit b multiplizieren erhalten wir

$$b = uab + vpb = [ab = cp] = ucp + vpb = (uc + vb) \cdot p.$$

Somit gilt $p \mid b$. □

Satz 10 (Zerlegung in Primfaktoren)**.** Jede natürliche Zahl $n > 1$ kann als Produkt von Primzahlen geschrieben werden. Die Primzahlen heißen *Primfaktoren* der Zahl n und sind bis auf die Reihenfolge eindeutig bestimmt.

Beweis. Wir zeigen die Existenz einer Zerlegung in Primfaktoren mittels vollständiger Induktion über n.
Für $n = 2$ ist n eine Primzahl.
Sei nun $n > 2$ und die Aussage richtig für alle natürlichen Zahlen, die kleiner als n sind. Dann ist n entweder eine Primzahl oder es gibt a, $b \in \mathbb{N}$ mit $0 < a, b < n$ so, dass $n = a \cdot b$ ist. Nach Induktionsannahme sind a und b Produkte von Primzahlen, also auch n.
Wir beweisen noch die Eindeutigkeit der Primfaktorzerlegung mittels Induktion über n.
Für $n = 2$ gibt es nur eine Darstellung.
Sei $n > 2$ und die Aussage richtig für alle natürlichen Zahlen n' mit $1 < n' < n$. Es seien

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k \text{ und } n = q_1 \cdot q_2 \cdot \ldots \cdot q_l$$

zwei Zerlegungen von n in Primfaktoren. Da die Primzahl p_1 die Zahl n teilt, muss p_1 auch das Produkt $q_1 \cdot q_2 \cdot \ldots \cdot q_l$ teilen. Nach Satz 9 teilt p_1 damit einen der Faktoren q_j mit $j \in \{1, \ldots, l\}$. Nach Umordnung von $q_1 \cdot q_2 \cdot \ldots \cdot q_l$ können wir annehmen, dass p_1 ein Teiler von q_1 ist. Da q_1 eine Primzahl ist, folgt $p_1 = q_1$. Nun können wir beide Darstellungen durch p_1 teilen und erhalten

$$n' = p_2 \cdot p_3 \cdot \ldots \cdot p_k \text{ und } n' = q_2 \cdot q_3 \cdot \ldots \cdot q_l.$$

Da $n' < n$ ist, sind die beiden Darstellungen nach Induktionsannahme gleich. Damit sind auch die Darstellungen von n gleich. □

1.5 Gruppen, Ringe und Körper

Definition (Gruppe)**.** Sei G eine Menge und $* : G \times G \to G : (a, b) \mapsto a * b$ eine Funktion. Das Paar $(G, *)$ heißt *Gruppe*, wenn folgende drei Bedingungen (*Gruppen-Axiome*) erfüllt sind:

(1) Für alle a, b, $c \in G$ ist $(a * b) * c = a * (b * c)$ (*Assoziativgesetz*).

(2) Es gibt ein Element $e \in G$ so, dass für alle $a \in G$ gilt: $a * e = e * a = a$ (e heißt *neutrales Element* von G).

(3) Für alle Elemente $a \in G$ gibt es ein $b \in G$ so, dass $a * b = b * a = e$ ist (b heißt zu a *inverses Element* und wird mit a^{-1} bezeichnet).

Eine Gruppe $(G, *)$ heißt *kommutativ* oder *abelsch*, wenn zusätzlich gilt:

(4) Für alle a, $b \in G$ ist $a * b = b * a$ (*Kommutativgesetz*).

Ist $(G, *)$ eine Gruppe, dann wird die Funktion $*$ als *Gruppenverknüpfung*, *Multiplikation* oder, wenn $(G, *)$ abelsch ist, als *Addition* bezeichnet. Wenn aus dem Zusammenhang ersichtlich ist, welche Verknüpfung auf G betrachtet wird, schreibt man statt $(G, *)$ kürzer G.

Beispiel. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}_{>0}, \cdot)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$ sind kommutative Gruppen. $(\mathbb{Z}, \cdot)$ ist keine Gruppe, da nicht jedes Element ein inverses Element besitzt, zum Beispiel besitzt 2 kein Inverses, da $\frac{1}{2} \notin \mathbb{Z}$.

Definition (Untergruppe)**.** Sei $(G, *)$ eine Gruppe mit neutralem Element e. Eine nichtleere Teilmenge $U \subset G$ heißt *Untergruppe* der Gruppe G (Schreibweise: $U \leq G$), wenn folgende Eigenschaften gelten:

(U1) Es existiert ein neutrales Element $e \in U$.

(U2) Ist $a \in U$, dann ist auch $a^{-1} \in U$.

(U3) $a, b \in U \Rightarrow a * b \in U$ (*Abgeschlossenheit*).

Bemerkung. Das neutrale Element $e \in U$ ist das gleiche neutrale Element $e \in G$ aus der Gruppe.

Beispiel. $\mathbb{Z} \leq \mathbb{Q}$, bezüglich der Addition ist $\mathbb{Z}$ eine Untergruppe von $\mathbb{Q}$.

Definition (Zyklische Gruppe)**.** Eine Gruppe G heißt *zyklisch*, wenn es ein $g \in G$ gibt, sodass sich jedes Element $h \in G$ in der Form $h = g^z$ mit $z \in \mathbb{Z}$ darstellen lässt. Ein Element g mit dieser Eigenschaft heißt ein *erzeugendes Element* von G.

Eine zyklische Gruppe mit erzeugendem Element g besteht also aus den Elementen

$$\langle g \rangle := \{g^i \mid i \in \mathbb{Z}\}.$$

Wenn die zyklische Gruppe additiv geschrieben wird, besteht sie aus den Elementen

$$\langle g \rangle := \{g \cdot i \mid i \in \mathbb{Z}\}.$$

Beispiel. Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch, denn das Element 1 erzeugt die gesamte Gruppe. Auch -1 ist ein erzeugendes Element von $(\mathbb{Z}, +)$. Damit gilt $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$.

Definition (Erzeugnis eines Elements)**.** Es sei G eine Gruppe und $g \in G$. Dann heißt $\langle g \rangle$ die von g *erzeugte Untergruppe* oder kurz das *Erzeugnis* von g.

Man kann auch sagen: Eine Gruppe G ist genau dann zyklisch, wenn sie von einem Element erzeugt werden kann, also wenn es ein $g \in G$ gibt mit $G = \langle g \rangle$.

Definition (Ring)**.** Sei R eine Menge und $+ : R \times R \to R$ sowie $\cdot : R \times R \to R$ Funktionen. Das Tripel $(R, +, \cdot)$ heißt ein *Ring*, wenn die folgenden Bedingungen (*Ring-Axiome*) erfüllt sind:

(1) $(R, +)$ ist eine abelsche Gruppe.

(2) Für alle $a, b, c \in R$ ist $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (*Assoziativgesetz*).

(3) Es gibt ein Element $e \in R$ so, dass für alle $a \in R$ gilt: $e \cdot a = a \cdot e = a$
(e heißt *Einselement*).

(4) Für alle a, b, $c \in R$ ist $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (*Distributivgesetz)*.

Ein Ring $(R, +, \cdot)$ heißt *kommutativ*, wenn zusätzlich gilt:

(5) Für alle a, $b \in R$ ist $a \cdot b = b \cdot a$ (*Kommutativgesetz*).

Ist $(R, +, \cdot)$ ein Ring, dann heißt $+$ die *Addition* und $\cdot$ die *Multiplikation* des Ringes. Das neutrale Element von $(R, +)$ heißt *Nullelement*. Das zu $a \in R$ bezüglich $+$ inverse Element wird mit $-a$ bezeichnet. Wenn aus dem Zusammenhang ersichtlich ist, welche Addition und Multiplikation auf der Menge R betrachtet werden, so schreibt man statt $(R, +, \cdot)$ kurz R.

Beispiel. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind kommutative Ringe.

Definition (Inverses Element)**.** Ein Element a eine Ringes R mit Einselement 1 ist *invertierbar*, wenn es ein Element $b \in R$ mit

$$a \cdot b = 1 = b \cdot a$$

gibt. Das Element b heißt dann zu a (bezüglich $\cdot$) *inverses Element* und wird mit a^{-1} bezeichnet.

Definition (Körper)**.** Sei K eine Menge und $+ : R \times R \to R$ sowie $\cdot : R \times R \to R$ Funktionen. Das Tripel $(K, +, \cdot)$ heißt ein *Körper*, wenn die folgenden Bedingungen erfüllt sind:

(1) $(K, +)$ ist eine abelsche Gruppe mit neutralem Element 0 und Inversem $-a$ von a.

(2) $(K \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe mit neutralem Element 1 und Inversem a^{-1} von a.

(3) Für alle a, b, $c \in R$ ist $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (*Distributivgesetz)*.

Zusammengefasst kann man sagen: Sei $(R, +, \cdot)$ ein kommutativer Ring mit mindestens zwei Elementen. R heißt ein *Körper*, wenn jedes Element von $R \setminus \{0\}$ invertierbar ist.

Beispiel. $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper. Der Ring $(\mathbb{Z}, +, \cdot)$ der ganzen Zahlen ist kein Körper, da nicht jedes Element ein multiplikatives Inverses besitzt. Zum Beispiel ist 3 nicht invertierbar, da $\frac{1}{3} \notin \mathbb{Z}$.

1.6 Rechnen mit Restklassen

Definition (Modulo)**.** Es seien $a, n \in \mathbb{Z}$ mit $n > 1$. Mit $a \; mod \; n$ (Sprechweise: a modulo n) bezeichnet man den kleinsten nichtnegativen Rest, der bei Division von a durch n entsteht.

Beispiel. $8 \bmod 5 = 3$, $14 \bmod 4 = 2$, $-4 \bmod 9 = 5$, $-250 \bmod 10 = 0$.

Definition (Kongruenz)**.** Es seien a, b, $n \in \mathbb{Z}$ mit $n > 1$. Man schreibt

$$a \equiv b \bmod n$$

(Sprechweise: a ist *kongruent* zu b modulo n), falls $a \bmod n = b \bmod n$ ist. Das heißt, dass die Reste von a und b nach Division durch n gleich sind.

Beispiel. $5 \equiv 11 \bmod 2$, da $5 \bmod 2 = 1$ und $11 \bmod 2 = 1$ sind.

Definition (Restklasse)**.** Es seien a, $n \in \mathbb{Z}$ mit $n > 1$. Dann heißt die Menge

$$\overline{a} := \{a + z \cdot n \mid z \in \mathbb{Z}\} = \{z \in \mathbb{Z} \mid z \bmod n = a \bmod n\} = \{z \in \mathbb{Z} \mid z \equiv a \bmod n\}$$

Restklasse von a modulo n. Die Restklasse $\overline{a}$ ist die Menge aller ganzen Zahlen, die bei Division durch n den gleichen Rest wie a ergeben. Man nennt die Zahl a auch einen *Repräsentanten* der Restklasse $\overline{a}$. Die Menge aller Restklassen modulo n

$$\{\overline{a} \mid a \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

wird mit

$$\mathbb{Z}_n \text{ oder } \mathbb{Z}/n\mathbb{Z}$$

bezeichnet. Sprechweise: $\mathbb{Z}$ modulo n.

Beispiel. Sei $n = 3$. Dann gibt es folgenden Restklassen:

$$\overline{0} = \{0 + z \cdot 3 \mid z \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\},$$
$$\overline{1} = \{1 + z \cdot 3 \mid z \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\} \text{ und}$$
$$\overline{2} = \{2 + z \cdot 3 \mid z \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}.$$

Die Menge aller Restklassen ist $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$. Betrachten wir zum Beispiel die Restklasse

$$\overline{5} = \{5 + z \cdot 3 \mid z \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}.$$

Das ist die Menge aller ganzen Zahlen, die bei Division durch 3 den Rest 2 ergeben. Das ist aber genau die Restklasse $\overline{2}$. Das bedeutet, dass auch 5 ein Repräsentant für die Restklasse $\overline{2}$ ist. Somit gilt in $\mathbb{Z}_3$, dass $\overline{5} = \overline{2}$ ist.

Satz 11 (Gleichheit von Restklassen)**.** Es seien a, b, $n \in \mathbb{Z}$ mit $n > 1$. Dann gilt

$$\overline{a} = \overline{b} \Leftrightarrow n \mid (b - a).$$

In Worten: Zwei Restklassen $\overline{a}$ und $\overline{b}$ sind genau dann gleich, wenn $(b - a)$ ein Vielfaches von n ist.

Beweis. „⇒": Sei $\overline{a} = \overline{b}$. Da b in der Restklasse $\overline{b}$ enthalten ist und die Restklasse $\overline{a}$ und $\overline{b}$ gleich sind, ist b auch in $\overline{a}$ enthalten. Das bedeutet, dass a und b bei Division durch n den gleichen Rest r haben. Es gibt also q_1 und $q_2 \in \mathbb{Z}$ mit

$$a = q_1 n + r \text{ und } b = q_2 n + r$$
$$\Rightarrow b - a = q_2 n + r - q_1 n - r = (q_2 - q_1)n$$

Also ist $b - a$ ein Vielfaches von n und damit durch n teilbar.
„⇐": Aus $n \mid (b - a)$ folgt $\exists t \in \mathbb{Z}$ mit $tn = b - a$. Daraus folgt $a = b - tn$ und $b = a + tn$. Um die Gleichheit von Mengen $\overline{a} = \overline{b}$ zu zeigen, müssen wir zeigen, dass $\overline{a} \subseteq \overline{b}$ und $\overline{b} \subseteq \overline{a}$ ist.
$\overline{a} \subseteq \overline{b}$: Sei $a' \in \overline{a}$ beliebig. Das bedeutet $a' = a + sn$ mit $s \in \mathbb{Z}$. Wegen $a = b - tn$ folgt

$$a' = a + sn = b - tn + sn = b + (-t + s)n \in \overline{b}.$$

Somit gilt $\overline{a} \subseteq \overline{b}$.
$\overline{b} \subseteq \overline{a}$: Sei $b' \in \overline{b}$. Das heißt $b' = b + zn$ mit $z \in \mathbb{Z}$. Aus $b = a + tn$ folgt

$$b' = b + zn = a + tn + zn = a + (t + z)n \in \overline{a}.$$

Somit ist $\overline{b} \subseteq \overline{a}$. Zusammen folgt $\overline{a} = \overline{b}$. □

Definition (Addition und Multiplikation von Restklassen)**.** Es sei $n \in \mathbb{Z}$ mit $n > 1$. Wir definieren die Addition und die Multiplikation wie folgt:

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n : (\overline{a}, \overline{b}) \mapsto \overline{a} + \overline{b} := \overline{a + b}$$
$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n : (\overline{a}, \overline{b}) \mapsto \overline{a} \cdot \overline{b} := \overline{a \cdot b}$$

In Worten: Zwei Restklassen werden addiert bzw. multipliziert, indem man die Repräsentanten addiert bzw. multipliziert und die entsprechende Restklasse bildet.

Satz 12. Die Addition und die Multiplikation von Restklassen sind wohldefiniert. Mit diesen Rechenoperationen ist $\mathbb{Z}_n$ ein kommutativer Ring mit n Elementen und heißt Restklassenring $\mathbb{Z}_n$.

Beweis. Um die Wohldefiniertheit der Addition und der Multiplikation zu überprüfen, müssen wir zeigen, dass die Rechenoperationen nicht von der Auswahl der Repräsentanten abhängig sind.
Seien a, c, b, $d \in \mathbb{Z}$, sodass $\overline{a} = \overline{c}$ und $\overline{b} = \overline{d}$. Dann sind nach Satz 11 $a - c$ und $b - d$ Vielfache von n, das heißt $a - c = kn$ und $b - d = hn$ für k, $h \in \mathbb{Z}$. Wir müssen zeigen, dass $\overline{a} + \overline{b} = \overline{c} + \overline{d}$ gilt. Nach Definition der Addition von Restklassen ist also zu zeigen, dass $\overline{a + b} = \overline{c + d}$ ist. Nach Satz 11 reicht es nachzuweisen, dass die Differenz $(a + b) - (c + d)$ ein Vielfaches von n ist.

$$(a + b) - (c + d) = (a - c) + (b - d) = kn + hn = (k + h)n$$

Wegen

$$ab - cd = ab - ad + ad - cd = a(b - d) + d(a - c) = ahn + dkn = (ah + dk)n$$

ist $ab - cd$ ein Vielfaches von n, also $\overline{ab} = \overline{cd}$.
Es kann nachgeprüft werden, dass die Addition und die Multiplikation von Restklassen

die Rechenregeln eines kommutativen Ringes erfüllen.[5] □

Satz 13. Es seien $a \neq 0$ und $n \geq 2$ ganze Zahlen. Die Restklasse $\overline{a} \in \mathbb{Z}_n$ ist genau dann invertierbar, wenn $ggT(a, n) = 1$ ist.

In diesem Fall wird $\overline{a}^{-1}$ wie folgt berechnet:

- Berechne mit dem erweiterten Euklidischen Algorithmus Zahlen u, $v \in \mathbb{Z}$ so, dass $u \cdot a + v \cdot n = 1$ ist.
- Dann ist $\overline{a}^{-1} = \overline{u}$.

Beweis. $\overline{a}$ ist invertierbar $\Leftrightarrow \exists u \in \mathbb{Z} : \overline{u} \cdot \overline{a} = \overline{1} \Leftrightarrow$ [addiere Vielfaches von n] $\Leftrightarrow$ $\exists u, v \in \mathbb{Z} : ua + vn = 1 \Leftrightarrow ggT(a, n) = 1$.

Berechne mit dem erweiterten Euklidischen Algorithmus u und v so, dass:

$$\overline{ua + vn} = \overline{ua} + \underbrace{\overline{vn}}_{\overline{0}} = \overline{1}.$$

So erhält man das zu $\overline{a}$ inverse Element $\overline{u}$. □

Satz 14. $\mathbb{Z}_n$ ist genau dann ein Körper, wenn n eine Primzahl ist.

Beweis. Der Ring $\mathbb{Z}_n$ ist genau dann ein Körper, wenn jedes Element aus $\mathbb{Z}_n \setminus \{0\}$ invertierbar ist. Dies ist genau dann der Fall, wenn alle Zahlen $1, 2, \ldots, n-1$ zu n teilerfremd sind, also wenn n eine Primzahl ist. □

Satz 15. Es seien a, $b \in \mathbb{Z}$ und p eine Primzahl. Dann ist in $\mathbb{Z}_p$

$$(\overline{a} + \overline{b})^p = \overline{a}^p + \overline{b}^p.$$

Beweis. Für $1 < k < p$ ist

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = p \cdot \frac{(p-1)!}{k!(p-k)!}.$$

Da p eine Primzahl ist und jede der Zahlen $1, 2, \ldots, k$ kleiner als p ist, wird $k!$ nach Satz 9 nicht von p geteilt. Aus dem gleichen Grund ist p kein Teiler von $(p-k)!$. Also muss

[5] Der Beweis wird in Beutelspacher und Zschiegner (2011) auf S. 86 und S. 88 beschrieben.

p ein Teiler von $\binom{p}{k}$ sein.
Nach dem Binomischen Lehrsatz gilt

$$(\overline{a}+\overline{b})^p = \sum_{k=0}^{p} \binom{p}{k} \overline{a}^k \overline{b}^{p-k}.$$

Da die Binomialkoeffizienten $\binom{p}{1}, \ldots, \binom{p}{p-1}$ alle durch p teilbar sind, bleiben modulo p nur die Summanden für $k = 0$ und $k = p$ übrig. Daher ist

$$(\overline{a}+\overline{b})^p = \binom{p}{0} \overline{a}^0 \overline{b}^p + \binom{p}{p} \overline{a}^p \overline{b}^0 = \overline{b}^p + \overline{a}^p.$$

□

Satz 16 (Kleiner Satz von Fermat)**.** Sei p eine Primzahl und $a \in \mathbb{Z}$. Dann ist

$$\overline{a}^p = \overline{a} \in \mathbb{Z}_p.$$

Wenn $\overline{a} \neq 0$ ist, dann gilt

$$\overline{a}^{p-1} = \overline{1} \in \mathbb{Z}_p.$$

Beweis. Die Aussage $\overline{a}^p = \overline{a}$ beweisen wir durch Induktion über a. Es genügt, den Satz für $a \geq 0$ zu zeigen, ansonsten ersetzen wir a durch eine kongruente nicht-negative Zahl.
Für $a = 0$ ist $\overline{a}^p = 0 = a$.
Sei nun $a > 0$. Nach Induktionsvoraussetzung (IV) ist $\overline{a}^p = \overline{a}$ und es gilt

$$(\overline{a+1})^p = (\overline{a}+\overline{1})^p \overset{\text{Satz 15}}{=} \overline{a}^p + \overline{1}^p \overset{\text{(IV)}}{=} \overline{a} + \overline{1} = \overline{a+1}.$$

Damit ist die Induktion abgeschlossen und der erste Teil des Satzes bewiesen.
Ist $\overline{a} \neq 0$ können wir $\overline{a}^p = \overline{a}$ durch a teilen und erhalten $\overline{a}^{p-1} = \overline{1}$. □

Beispiel. Es sei p eine Primzahl, $a \in \mathbb{Z}$, die nicht von p geteilt wird und e eine große natürliche Zahl. Mit Satz 16 kann der Rest von a^e nach Division durch p schnell berechnet werden. Dividiere zuerst e mit Rest durch $p-1$:

$$e = m \cdot (p-1) + r.$$

Dann ist

$$\overline{a}^e = \overline{a}^{m\cdot(p-1)+r} = (\overline{a}^{p-1})^m \cdot \overline{a}^r = \overline{1}^m \cdot \overline{a}^r = \overline{1} \cdot \overline{a}^r = \overline{a}^r \in \mathbb{Z}_p.$$

Sei zum Beispiel $p = 13$, $a = 7$ und $e = 10000$. Dann ist $10000 = 833 \cdot 12 + 4$ und somit

$$\overline{7}^{10000} = (\overline{7}^{12})^{833} \cdot \overline{7}^4 = \overline{1}^{833} \cdot \overline{7}^4 = \overline{7}^4 = (\overline{7}^2)^2 = \overline{49}^2 = \overline{-3}^2 = \overline{9} \in \mathbb{Z}_{13}.$$

2 Kryptologie

Kryptographie ist die Wissenschaft von der Verschlüsselung einer Mitteilung oder von der Verschleierung des Inhaltes einer Mitteilung. Unter **Kryptoanalyse** versteht man sowohl die Wissenschaft von der unbefugten Entschlüsselung von Nachrichten ohne Kenntnis des Schlüssels, als auch die Analyse kryptographischer Verfahren zum Zweck der Bewertung ihrer Sicherheit[1]. Beide Wissenschaften zusammen bilden die **Kryptologie**, die Wissenschaft von der Verschlüsselung in allen ihren Formen. Manchmal wird der Begriff Kryptographie für Kryptologie verwendet und bezeichnet alles, was mit Ver- und Entschlüsselungen zu tun hat.

Bei der Übermittlung von geheimen Nachrichten ist zwischen **Steganographie** und Kryptographie zu unterscheiden. Ziel der Steganographie ist es, die Existenz einer Botschaft zu verbergen. Ein Beispiel hierfür ist der Gebrauch von unsichtbarer Tinte, wie die Milch der Thtihymallus-Pflanze, die nach dem Trocknen durchsichtig ist und durch Erhitzen sichtbar gemacht werden kann.[2] Bei der Kryptographie hingegen, wird der Sinn einer Nachricht, mittels eines Verfahrens der Verschlüsselung, verborgen. Sie wird für einen unbefugten Dritten unleserlich gemacht, ohne deren Existenz zu verschleiern.

Ein **Klartext** ist die ursprüngliche Mitteilung vor der Verschlüsselung. Durch die Wahl eines **Schlüssels** wird ein allgemeines Verfahren zur Verschlüsselung (Algorithmus) festgelegt. Wird der Schlüssel und der Algorithmus auf einen Klartext angewendet, erhält man die verschlüsselte Nachricht, welche auch **Geheimtext** oder **Chiffre** genannt wird. Der Empfänger kann den Geheimtext, mit dem ihm bekannten Schlüssel und dem Algorithmus, entschlüsseln, d.h. in den Klartext zurückverwandeln (vgl. Abbildung 1).

[1] Vgl. Horster (1985), S. 14

[2] In dieser Arbeit wird auf Steganographie nicht weiter eingegangen und auf weiterführende Literatur (z.B. Bauer (1997)) verwiesen.

Abbildung 1: Verhältnis von Algorithmus und Schlüssel[3]

Verwenden Sender und Empfänger zum **Chiffrieren** (Verschlüsseln) und zum **Dechiffrieren** (Entschlüsseln) den gleichen Schlüssel, spricht man von einer **symmetrischen** Verschlüsselung. Sind Chiffrier- und Dechiffrierschlüssel hingegen unterschiedlich, handelt es sich um eine **asymmetrische** Verschlüsselung.

2.1 Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung müssen Sender und Empfänger, vor der Übertragung einer Nachricht, den Schlüssel auf einem sicheren Weg ausgetauscht haben. Mit diesem Schlüssel verschlüsselt der Sender den Klartext und schickt den Geheimtext an den Empfänger. Der Empfänger kann den Geheimtext mit dem vereinbarten Schlüssel entschlüsseln. Sender und Empfänger benutzen also denselben Schlüssel zum Ver- und Entschlüsseln der Nachricht.

Man unterscheidet bei der symmetrischen Verschlüsselung zwischen zwei Verfahren, die Transposition und die Substitution.

[3]Singh (2002), S. 27

2.1.1 Transposition

Die Transposition bezeichnet ein Verfahren, bei dem die Buchstaben des Klartextes neu angeordnet werden. Jeder Buchstabe der ursprünglichen Nachricht bleibt erhalten und ändert nur die Position in der er Auftritt. Mathematisch kann die Transpositionschiffre als eine Permutation der Stellen des Klartextes beschrieben werden.

Das Verfahren ist bei sehr kurzen Mitteilungen relativ unsicher, weil die Anzahl der Möglichkeiten, die Buchstaben umzustellen, begrenzt ist. Betrachten wir zum Beispiel ein Wort mit drei Buchstaben, sehen wir, dass es auf sechs verschiedene Weisen angeordnet werden kann: UND, UDN, DUN, DNU, NUD und NDU. Die Anzahl der möglichen Anordnungen ist 3!. Für n Buchstaben gibt es $n!$ verschiedene Möglichkeiten, sie neu anzuordnen[4]. Bei einer Nachricht mit 34 Buchstaben, das heißt $34! \approx 2.9 \cdot 10^{38}$ verschiedenen Anordnungsmöglichkeiten, wäre es unmöglich, manuell alle Möglichkeiten durchzuprüfen. Eine Zufallstransformation scheint eine perfekte Verschlüsselungsmethode zu sein, weil es für einen Unbefugten unmöglich wäre, die Nachricht zu entschlüsseln. Das Problem ist aber, dass auch der eigentliche Empfänger nicht in der Lage sein wird, die Nachricht wiederherzustellen, wenn die Buchstaben ohne Sinn durcheinandergewürfelt wurden. Deswegen müssen Sender und Empfänger zuvor vereinbaren, nach welchem System die Buchstaben umgestellt werden.

Das bekannteste Transpositionsverfahren ist die Skytale, die im Folgenden näher betrachtet wird.

Skytale

Die Skytale ist das erste militärische Kryptographie-Verfahren und wurde bereits im 5. Jahrhundert v. Chr. von den Spartanern verwendet, um geheime Botschaften zu übermitteln. Zum Verfassen einer Nachricht wickelte der Sender spiralförmig einen Leder- oder Pergamentstreifen um eine Skytale (Holzstab) und schrieb die Nachricht, ohne Leer- und Satzzeichen, der Länge des Stabes nach auf den Streifen. Wurde der Streifen dann abgewickelt, konnte die Nachricht nicht mehr gelesen werden, da es nur eine sinnlose Aneinanderreihung von Buchstaben enthielt (vgl. Abbildung 2). Der Geheimtext

[4] Siehe Satz 1

konnte nur entschlüsselt werden, indem der Lederstreifen um eine Skytale mit demselben Durchmesser gewickelt wurde. Bei diesem Verfahren ist der geheime Schlüssel der Durchmesser der Skytale.

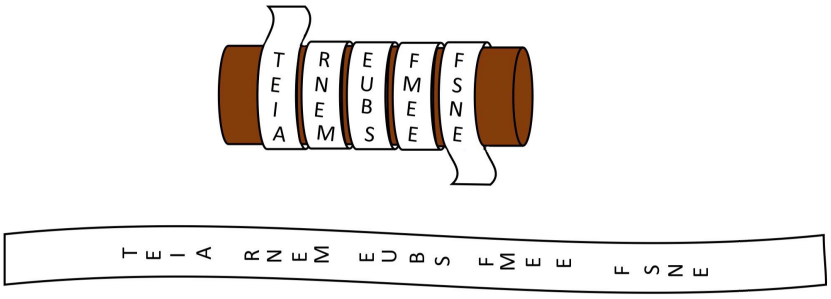


Abbildung 2: Eine Skytale und der abgerollte Papierstreifen.

In Abbildung 2 wird die Nachricht mit einer Skytale wie folgt verschlüsselt:

```
Klartext:   TREFFEN UM SIEBEN AM SEE
Geheimtext: TEIA RNEM EUBS FMEE FSNE
```

Wir können die Nachricht auch ohne Holzstab entschlüsseln, wenn wir den Umfang der Skytale durch die Anzahl der Buchstaben ausdrücken, die einmal um die Skytale herum passen, das entspricht der Anzahl der Zeilen des Klartextes auf dem Holzstab. Schreiben wir den Klartext zeilenweise in u Zeilen, erhalten wir den Geheimtext, indem wir die Buchstaben spaltenweise ablesen. Um den Geheimtext zu entschlüsseln, schreiben wir diesen ebenfalls in u Zeilen an, diesmal aber spaltenweise und lesen die Buchstaben zeilenweise ab.

In unserem Beispiel ist der Umfang $u = 4$ und die Nachricht besteht insgesamt aus 20 Buchstaben. Also müssen wir pro Zeile 5 Buchstaben anschreiben, um die gesamte Nachricht auf 4 Zeilen aufteilen zu können. Wir erhalten eine Tabelle mit 4 Zeilen und 5 Spalten:

```
  T  R  E  F  F
  E  N  U  M  S
↓ I  E  B  E  N
  A  M  S  E  E
```

Spaltenweise von oben nach unten ausgelesen, erhalten wir den zuvor angegebenen Geheimtext.

Haben wir zum Beispiel folgenden Geheimtext abgefangen, können wir diesen, ohne die dazugehörige Skytale, indem wir verschiedene Umfänge u ausprobieren, entschlüsseln:

```
Geheimtext: DHRKTSIRDYSEEIETCLSCOAHTEHHLLNTNEUAWEEECUSNS
```

Wählen wir zum Beispiel $u = 5$, erhalten wir keine sinnvolle Nachricht:

```
D  S  S  T  O  H  T  W  U
H  I  E  C  A  H  N  E  S
R  R  E  L  H  L  E  E  N
K  D  I  S  T  L  U  E  S
T  Y  E  C  E  N  A  C
```

Verwenden wir hingegen $u = 6$, und lesen zeilenweise ab, erhalten wir folgende Botschaft:

```
D  I  E  S  E  N  A  C
H  R  I  C  H  T  W  U
R  D  E  O  H  N  E  S
K  Y  T  A  L  E  E  N
T  S  C  H  L  U  E  S
S  E  L  T
```

```
Klartext:   DIESE NACHRICHT WURDE OHNE SKYTALE ENTSCHLUESSELT
```

Werden die Buchstaben des Klartextes durchnummeriert, kann die Verschlüsselung auch als Permutation dargestellt werden. Wird die Permutation auf den Klartext angewendet, erhält man den Geheimtext.

Die Permutation für die Verschlüsselung in Abbildung 2 sieht wie folgt aus:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 1 & 6 & 11 & 16 & 2 & 7 & 12 & 17 & 3 & 8 & 13 & 18 & 4 & 9 & 14 & 19 & 5 & 10 & 15 & 20 \end{pmatrix}$$

Das bedeutet, dass der erste Buchstabe der Nachricht auf den ersten Buchstaben abgebildet wird, der zweite Buchstabe auf den 6. Buchstaben, usw., wobei die Klartextbuchstaben wir folgt nummeriert werden:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
T	R	E	F	F	E	N	U	M	S	I	E	B	E	N	A	M	S	E	E

Entschlüsselt wird mit der Umkehrpermutation[5]

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 1 & 5 & 9 & 13 & 17 & 2 & 6 & 10 & 14 & 18 & 3 & 7 & 11 & 15 & 19 & 4 & 8 & 12 & 16 & 20 \end{pmatrix},$$

wobei diesmal zuvor die Geheimtextbuchstaben aufsteigend nummeriert werden. Der erste Buchstabe bleibt der erste, der zweite bzw. dritte Buchstabe des Klartextes ist der 5. bzw. 9. Buchstabe des Geheimtextes, usw.

2.1.2 Substitution

Im Gegensatz zur Transposition wird bei der Substitution jeder Buchstabe im Klartext durch einen anderen Buchstaben oder ein Symbol ersetzt, wobei die Reihenfolge der Zeichen erhalten bleibt.

Auch bei der Substitution müssen Sender und Empfänger zuvor vereinbaren, durch welche Zeichen die Buchstaben des Klartextes ersetzt werden. Diese Folge von Zeichen wird **Geheimtextalphabet** genannt. Das **Klartextalphabet** ist das Alphabet, mit dem der Klartext geschrieben ist. Wie in der Kryptographie üblich, werden im Folgenden das Klartextalphabet und der Klartext in Kleinbuchstaben, das Geheimtextalphabet und der Geheimtext in Großbuchstaben geschrieben.

[5] Angepasst von Horster (1985), S. 73

Ein Substitutionsverfahren, bei dem genau ein Geheimtextalphabet eingesetzt wird, wird als **monoalphabetische Verschlüsselung** bezeichnet. Ein Klartextbuchstabe wird immer mit demselben Buchstaben[6] des Geheimtextalphabets verschlüsselt. Verwendet man hingegen mehrere Geheimtextalphabete für eine Nachricht, handelt es sich um eine **polyalphabetische Verschlüsselung**. Da das Geheimtextalphabet während der Verschlüsselung wechselt, werden gleiche Klartextbuchstaben meistens mit unterschiedlichen Geheimtextbuchstaben verschlüsselt, je nachdem, welches Geheimtextalphabet gerade verwendet wird.

Caesar-Verschiebung

Die Caesar-Verschiebung ist eine einfache monoalphabetische Substitution, die von Gaius Julius Caesar (100 bis 44 v. Chr.) eingesetzt wurde. Jeder Buchstabe der Nachricht wird durch den Buchstaben, der im Alphabet drei Stellen weiter folgt, ersetzt. Dabei geht es nach Z mit A weiter. Das Geheimtextalphabet erhält man, wenn man das Klartextalphabet um 3 Stellen nach links versetzt.

Klartextalphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheimtextalphabet	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Eine Botschaft wird chiffriert, indem der Buchstabe des Klartextes durch den darunter stehenden Geheimtextbuchstaben ersetzt wird.

Klartext	c	a	e	s	a	r	v	e	r	s	c	h	i	e	b	u	n	g
Geheimtext	F	D	H	V	D	U	Y	H	U	V	F	K	L	H	E	X	Q	J

Zum Dechiffrieren wird jeder Geheimtextbuchstaben durch den darüberstehenden Klartextbuchstaben ersetzt. Der Schlüssel ist das Geheimtextalphabet bzw. die Anzahl der Stellen, um die das Alphabet verschoben wird.

Die Caesar-Verschiebung kann auch verallgemeinert werden, wenn statt einer festen Verschiebung um drei Stellen, das Geheimtextalphabet um eine beliebige Anzahl von Stellen verschoben wird. Da unser Alphabet aus 26 Buchstaben besteht, kann man es um bis zu

[6] Das Geheimtextalphabet kann auch aus beliebigen Symbolen oder Zeichen bestehen, in dieser Arbeit beschränken wir uns aber auf das deutsche Alphabet mit 26 Buchstaben.

25 Stellen verschieben und erhält somit 25 verschiedene Schlüssel, mit denen Nachrichten verschlüsselt werden können.

Mathematisch kann die Caesar-Verschiebung wie folgt beschrieben werden. Man ordnet jedem Buchstaben des Klartextalphabets die Zahlen 0 bis 25 zu.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Dann kann man einen Klartextbuchstaben x mit der Verschlüsselungsfunktion

$$V(x) = x + k \bmod 26$$

verschlüsseln und erhält den Geheimtextbuchstaben $c = V(x)$, wobei k der geheime Schlüssel ist. Die Entschlüsselung erfolgt durch die Umkehrung der Berechnungen, die für die Verschlüsselung verwendet wurden. Dies entspricht der Entschlüsselungsfunktion

$$V^{-1}(c) =: E(c) = c - k \bmod 26.$$

Für ein n-elementiges Alphabet kann man die Caesar-Verschlüsselung durch die Funktionen

$$V(x) = x + k \bmod n \text{ und } E(c) = c - k \bmod n$$

auf der Menge $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ beschreiben.

Im folgenden Beispiel wird der Klartext „Kryptologie" mit dem Schlüssel $k = 11$ verschlüsselt.

Klartext	k	r	y	p	t	o	l	o	g	i	e
Klartext in Zahlen	10	17	23	15	19	14	11	14	6	8	4
+ Schlüssel	11	11	11	11	11	11	11	11	11	11	11
Summe	21	28	24	26	30	25	22	25	17	19	15
modulo 26	21	2	24	0	4	25	22	25	17	19	15
Geheimtext	V	C	Y	A	E	Z	W	Z	R	T	P

Der Grundsatz der Kryptologie, welche durch das **Prinzip von Kerckhoffs** beschrieben

wird, besagt folgendes: „Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels.“[7] Also muss man davon ausgehen, dass der Gegner weiß, mit welchem Verfahren verschlüsselt wurde. Wenn ein Angreifer weiß oder vermutet, dass eine Nachricht mit einer Caesar-Verschiebung verschlüsselt wurde, kann er den Geheimtext sehr leicht knacken, indem er systematisch alle möglichen Schlüssel durchprobiert. Das bedeutet, dass er höchstens 25 Versuche benötigt. Diese Methode, eine Chiffre zu brechen, ist die **systematische Schlüsselsuche**. Man nennt diesen Angriff auch Exhaustionsmethode oder Brute-Force-Attack (Methode der rohen Gewalt). Wie man gut sehen kann, ist allein die Geheimhaltung des Schlüssels nicht ausreichend, um die Sicherheit eines Verschlüsselungssystems zu gewährleisten. Man benötigt auch eine hohe Anzahl möglicher Schlüssel.

Allgemeine monoalphabetische Substitution

Die Anzahl der Schlüssel kann erhöht werden, indem man die alphabetische Reihenfolge des Geheimtextalphabets aufhebt und eine beliebige Permutation des Klartextalphabets zulässt.

Klartextalphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheimtextalphabet	J	L	P	A	W	I	Q	B	C	T	R	Z	Y	D	S	K	E	G	F	X	H	U	O	N	V	M

Für das Standardalphabet aus 26 Buchstaben gibt es dann $26! \approx 4 \cdot 10^{26}$ mögliche Permutationen[8]. Also gibt es insgesamt $26! - 1$ verschiedene Schlüssel, wenn man eine Möglichkeit, welche dem Klartextalphabet entspricht, subtrahiert. Die Anzahl der möglichen Schlüssel ist so groß, dass es selbst mit den schnellsten Computern in realistischer Zeit nicht möglich wäre, alle Schlüssel durchzuprobieren[9]. Heute ist eine systematische Schlüsselsuche im Bereich von 10^{16} Schlüsseln realistisch[10].

Die Verschlüsselung ist leicht anwendbar, man kann sich aber das Geheimtextalphabet schwer merken. Das Geheimtexalphabet sollte aber einfach sein, da sich Sender und Empfänger über diesen Schlüssel verständigen müssen.

[7] Beutelspacher (2009), S. 15
[8] Siehe Satz 1
[9] Vgl. Freiermuth et al. (2010), S. 76
[10] Vgl. Beutelspacher et al. (2010), S. 14

Schlüsselwort-Chiffre

Eine weiter Möglichkeit der monoalphabetischen Substitution, mit einfach zu merkendem Geheimtextalphabet, aber immer noch vielen Schlüsseln, ist die Schlüsselwort-Chiffre. Es wird ein beliebiges Schlüsselwort oder ein Schlüsselsatz festgelegt. Das Geheimtextalphabet wird erzeugt, indem man das Schlüsselwort, ohne Buchstabenwiederholung, als Anfang des Geheimtextalphabets schreibt und, beginnend mit dem letzten Buchstaben des Schlüsselworts, mit dem restlichen Alphabet in der üblichen Reihenfolge auffüllt. Die bereits im Schlüsselwort vorgekommenen Buchstaben werden dabei weggelassen.

Wir wählen zum Beispiel als Schlüsselwort „Julius Caesar“. Entfernen wir alle Leerzeichen und die wiederholten Buchstaben, ergibt sich die Buchstabenfolge „JULISCAER“ und das Geheimtextalphabet sieht wie folgt aus:

```
Klartextalphabet    a b c d e f g h i j k l m n o p q r s t u v w x y z
Geheimtextalphabet  J U L I S C A E R T V W X Y Z B D F G H K M N O P Q
```

Der Vorteil dieser Verschlüsselung ist, dass man sich nur das Schlüsselwort merken muss, um das ganze Geheimtextalphabet zu erhalten.

Die Einfachheit und die große Anzahl möglicher Schlüssel machte die Schlüsselwort-Chiffre jahrhundertelang zum bevorzugten Verschlüsselungssystem. Doch einem arabischen Gelehrten des neunten Jahrhunderts gelang es, ein Verfahren zu entwickeln, das die monoalphabetische Verschlüsselung brechen konnte. Mit diesem Verfahren, auch als **Häufigkeitsanalyse** bezeichnet, muss man nicht mehr alle möglichen Schlüssel durchprobieren. Der Geheimtext kann durch die Analyse der Häufigkeiten der Buchstaben entschlüsselt werden.

Häufigkeitsanalyse

In jeder natürlichen Sprache kommen einige Buchstaben häufiger vor als andere. Da bei der monoalphabetischen Verschlüsselung jeder Klartextbuchstabe mit demselben Geheimtextbuchstaben verschlüsselt wird, bleibt die Häufigkeitsverteilung der Buchstaben erhalten, nur sind die einzelnen Häufigkeiten anderen Buchstaben zugeordnet. Bestimmt man also die Anzahl der einzelnen Buchstaben eines Geheimtextes, wird der häufigste

Buchstabe höchstwahrscheinlich dem Buchstaben entsprechen, der in dieser Sprache am meisten verwendet wird. Die weiteren Buchstaben lassen sich ebenfalls entsprechend ihrer Häufigkeit den jeweiligen Buchstaben zuordnen. Betrachtet man zusätzlich die Häufigkeiten von Bigrammen, Zweierkombinationen von Buchstaben, und Trigrammen, Dreierkombinationen von Buchstaben, kann man eine monoalphabetisch verschlüsselte Nachricht relativ einfach durch die Häufigkeitsanalyse entschlüsseln. Man muss allerdings wissen, in welcher Sprache die Nachricht verfasst wurde, da die Buchstaben, je nach Sprache, unterschiedlich oft vorkommen.

In der deutschen Sprache ist das `e` mit $17,4\%$ am häufigsten vertreten, gefolgt von den Buchstaben `n` mit $9,78\%$ und `i` mit $7,55\%$. Die relativen Häufigkeiten der Buchstaben sind in Tabelle 1 aufgelistet, dabei wurden Leer-und Satzzeichen nicht berücksichtigt und die Umlaute `ä`, `ö`, `ü` wie `ae`, `oe`, `ue` behandelt.

Buchstabe	Häufigkeit in %	Buchstabe	Häufigkeit in %
a	6,51	n	9,78
b	1,89	o	2,51
c	3,06	p	0,97
d	5,08	q	0,02
e	17,40	r	7,00
f	1,66	s	7,27
g	3,01	t	6,15
h	4,76	u	4,35
i	7,55	v	0,67
j	0,27	w	1,89
k	1,21	x	0,03
l	3,44	y	0,04
m	2,53	z	1,13

Tabelle 1: Häufigkeiten der Buchstaben in deutschsprachigen Texten[11]

Weniger verlässlich ist diese Analyse bei Texten, die weniger als hundert Buchstaben haben, weil kurze Texte häufig von der gewöhnlichen Verteilung der Buchstaben der je-

[11] Vgl. Beutelspacher (2009), S. 8

weiligen Sprache abweichen. Außerdem gibt es auch Texte, deren Buchstabenhäufigkeit sich deutlich von der Häufigkeit der Buchstaben innerhalb der jeweiligen Sprache unterscheidet. Als Beispiel kann man hier den folgenden Zungenbrecher anführen: „In Ulm und um Ulm und um Ulm herum“[12]. Diese lassen sich durch Häufigkeitsanalyse nicht entschlüsseln.

Wir werden die Anwendung der Häufigkeitsanalyse nun an einem Beispiel verdeutlichen. Nehmen wir an, wir hätten den folgenden Geheimtext abgefangen, von dem wir wissen oder vermuten, dass er mittels monoalphabetischer Substitution verschlüsselt wurde und in deutscher Sprache verfasst ist[13]:

> PR ISRSQ YSPUD SYOCREBS GPS NFRZB GSY NCYBVEYCWDPS SPRS ZVOUDS HVOONVQQSRDSPB, GCZZ GPS NCYBS SPRSY SPRMPESR WYVHPRM GSR YCFQ SPRSY ECRMSR ZBCGB SPRRCDQ FRG GPS NCYBS GSZ YSPUDZ GSR SPRSY WYVHPRM. QPB GSY MSPB ASTYPSGPEBSR GPSZS FSASYQCSZZPE EYVZZSR NCYBSR RPUDB OCSRESY, FRG QCR SYZBSOOBS SPRS NCYBS GSZ YSPUDZ, GPS ESRCF GPS EYVSZZS GSZ YSPUDZ DCBBS.
>
> AVYESZ, HVR GSY ZBYSRES GSY JPZZSRZUDCTB

Als Erstes zählen wir, wie oft jeder Buchstabe im Geheimtext enthalten ist und erstellen eine Häufigkeitstabelle (mit oder ohne relative Häufigkeiten):

[12] Singh (2002), S. 36f.
[13] Vgl. Singh (2002), S. 38-42

Buchstabe	Häufigkeit	in %	Buchstabe	Häufigkeit	in %
A	3	0,92	N	7	2,14
B	20	6,12	O	7	2,14
C	18	5,50	P	30	9,17
D	11	3,36	Q	8	2,45
E	12	3,67	R	32	9,79
F	6	1,83	S	67	20,49
G	20	6,12	T	2	0,61
H	4	1,22	U	7	2,14
I	1	0,31	V	10	3,06
J	1	0,31	W	3	0,92
K	0	0	X	0	0
L	0	0	Y	29	8,87
M	5	1,53	Z	24	7,34

Wir betrachten die fünf häufigsten Buchstaben S, R, P, Y und Z. Da alles auf Statistik beruht, können wir nicht mit Sicherheit sagen, dass die Buchstaben eins zu eins mit der Häufigkeitsverteilung in Tabelle 1 zusammenpassen. Wir können aber sehen, dass der Buchstabe S etwa doppelt so oft vorkommt wie R und können deswegen davon ausgehen, dass S für den mit Abstand häufigsten Buchstaben in der deutschen Sprache, nämlich e steht. Nun vermuten wir, dass es sich bei den nächsten vier Buchstaben R, P, Y und Z um die zweit- bis fünfthäufigsten Buchstaben n, i, s und r im Deutschen handelt, aber wir wissen nicht, in welcher Reihenfolge. Wir verfeinern die Häufigkeitsanalyse und betrachten die häufigsten Bigramme der deutschen Sprache (vgl. Tabelle 2).

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

Tabelle 2: Die häufigsten Bigramme in deutschsprachigen Texten[14]

Nun nehmen wir unseren mutmaßlichen Geheimtextbuchstaben für e, also S, und zählen, wie viele Bigramme mit den zweit- bis fünfthäufigsten Buchstaben R, P, Y und Z auftreten:

Bigramme	Häufigkeit
RS/SR	6/13
PS/SP	8/13
YS/SY	5/11
ZS/SZ	4/7

Wir können davon ausgehen, dass die drei häufigsten Bigramme SR, SP und SY den häufigsten Bigrammen mit e in deutschsprachigen Texten en, er und ei entsprechen. Die zwei weniger häufigen Bigramme ZS und SZ stehen wahrscheinlich für se und es. Wir verfeinern noch einmal die Analyse und suchen nach dem im Deutschen häufigsten Trigramm ein (vgl. Tabelle 3), damit wir herausfinden, welche Geheimtextbuchstaben für n und i stehen. Wir zählen im Geheimtext, wie oft Trigramme mit S und einer Zweierkombination der Buchstaben R, P und Y vorkommen. Es kommt siebenmal SPR vor, wobei SRP, SRY, SYR, SPY und SYP überhaupt nicht aufreten. Deshalb können wir annehmen, dass P für i und R für n steht. Nun möchten wir feststellen, ob die verbleibenden häufigen Buchstaben Y und Z für s und r oder für r und s stehen. Dazu werden wir zuerst d ausfindig machen und danach mit dem Wissen, dass der viel öfter vorkommt als des, die

[14] Vgl. Beutelspacher (2009), S. 17

Trigramm	Häufigkeit in %	Trigramm	Häufigkeit in %
ein	1,14	nde	0,70
ich	1,12	cht	0,67
der	0,92	ine	0,57
sch	0,84	den	0,55
und	0,81	end	0,54
die	0,74	che	0,52

Tabelle 3: Die häufigsten Trigramme in deutschsprachigen Texten[15]

Buchstaben zuorden. Da im Geheimtext die Wortzwischenräume beibehalten wurden, können wir nach dem häufigsten Wort im Deutschen, nämlich `ein` suchen. Wir wissen bereits, dass `PS` für `ie` steht und finden im Geheimtext fünfmal das Einzelwort `GPS`. Das bedeutet, dass es sich bei `G` um `d` handeln muss. Wir zählen jetzt die Häufigkeiten von `der` und `des`, also im Geheimtext `GSY` und `GSZ`, um `r` und `s` unterscheiden zu können. `GSY` tritt viermal und `GSZ` dreimal auf. Vergleichen wir zusätzlich noch eimal die Bigramme `SY` und `SZ` sehen wir, dass `SY` öfter vorkommt als `SZ` und können unsere Vermutung, dass `Y` für `r` und `Z` für `s` steht, festigen. Damit haben wir sechs Buchstaben mit hoher Wahrscheinlichkeit richtig entschlüsselt und können die Geheimtextbuchstaben durch die ensprechenden Klartextbuchstaben ersetzten:

```
in IeneQ reiUD erOCnEBe die NFnsB der NCrBVErCWDie eine sVOUDe
HVOONVQQenDeiB, dCss die NCrBe einer einMiEen WrVHinM den rCFQ ei-
ner ECnMen sBCdB einnCDQ Fnd die NCrBe des reiUDs den einer WrVHinM.
QiB der MeiB AeTriediEBen diese FeAerQCessiE ErVssen NCrBen niUDB
OCenEer, Fnd QCn ersBeOOBe eine NCrBe des reiUDs, die EenCF die Er-
Vesse des reiUDs DCBBe.
                                    AVrEes, HVn der sBrenEe der JissensUDCTB
```

Mit diesem teilentschlüsselten Text können wir versuchen, ein paar der anderen Buchstaben zu erraten. Wir finden zum Beispiel das Wort `reiUD`, das Klarwort wird `reich` ergeben, weil `e` und `n` bereits vergeben sind. Und `dCss` wird höchstwahrscheinlich `dass` bedeuten. Wir setzten auch diese Buhstaben ein und bekommen:

```
in IeneQ reich erOanEBe die NFnsB der NarBVEraWhie eine sVOche
```

[15] Vgl. Wätjen (2018), S. 352

> HVOONVQQenheiB, dass die NarBe einer einMiEen WrVHinM den raFQ einer EanMen sBadB einnahQ Fnd die NarBe des reichs den einer WrVHinM. QiB der MeiB AeTriediEBen diese FeAerQaessiE ErVssen NarBen nichB OaenEer, Fnd Qan ersBeOOBe eine NarBe des reichs, die EenaF die ErVesse des reichs haBBe.
>
> AVrEes, HVn der sBrenEe der JissenschaTB

Wir können weitere Buchstaben erraten. Durch die Wörter sBadB und nichB können wir sagen, dass das B für t steht. Das letzte Wort wird vermutlich wissenschaft lauten. Wir könnten so weitermachen oder auch zusammenfassen, was wir über das Geheimtextalphabet bereits wissen, vielleicht können wir den Schlüssel bereits erkennen.

Klartextalphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheimtextalphabet	C	-	U	G	S	T	-	D	P	-	-	-	-	R	-	-	-	Y	Z	B	-	-	J	-	-	-

Wir sehen, dass der Schlüssel ziehmlich sicher aus einem Schlüsselwort besteht, da die Buchstaben Y, Z und B hintereinander vorkommen. Man kann jetzt einerseits noch ein paar Buchstaben raten, zum Beispiel könnte Fnd und heißen und einnahQ steht wahrscheinlich für einnahm. Andererseits könnten wir erkennen, dass das Schlüsselwort der Name eines Roman-Detektivs aus einer Erzählung von Edgar Allan Poe ist: C. Auguste Dupin. Nun können wir das gesamte Geheimtexalphabet erstellen und bekommen den vollständigen Klartext:

Klartextalphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheimtextalphabet	C	A	U	G	S	T	E	D	P	I	N	O	Q	R	V	W	X	Y	Z	B	F	H	J	K	L	M

> In jenem Reich erlangte die Kunst der Kartographie eine solche Vollkommenheit, dass die Karte einer einzigen Provinz den Raum einer ganzen Stadt einnahm und die Karte des Reichs den einer Provinz. Mit der Zeit befriedigten diese uebermaessig grossen Karten nicht laenger, und man erstellte eine Karte des Reichs, die genau die groesse des Reichs hatte.
>
> Borges, Von der Strenge der Wissenschaft

Obwohl monoalphabetische Verschlüsselungsverfahren eine so große Anzahl möglicher Schlüssel haben, dass das systematische Durchprobieren aller Schlüssel aussichtslos ist,

können diese Verfahren durch eine Häufigkeitsanalyse leicht geknackt werden, wenn der Text genügend lang ist. Verwendet man die Häufigkeitsanalyse bei der Caesar-Verschiebung, genügt es, den häufigsten Buchstaben im Geheimtext zu bestimmen und diesen mit dem Buchstaben zu identifizieren, der in dieser Sprache am meisten verwendet wird. Damit weiß man, um wie viele Stellen das Klartextalphabet verschoben wurde und erhält das Geheimtextalphabet.

Die größte Schwäche der monoalphabetischen Verschlüsselung beruht darauf, dass die Häufigkeit der Buchstaben erhalten bleibt, diese nur anderen Buchstaben zugeordnet werden. Um diese Schwäche zu beheben, wurden polyalphabetische Verschlüsselungsverfahren entwickelt. Bei diesen Verfahren werden mehrere Geheimtextalphabete im Wechsel benutzt, was dazu führt, dass gleiche Klartextbuchstaben mit unterschiedlichen Geheimtextbuchstaben verschlüsselt werden. Somit unterscheiden sich die Häufigkeiten der einzelnen Geheimtextbuchstaben von den Häufigkeiten der Klartextbuchstaben.[16]

Vigenère-Verschlüsselung

Die Vigenère-Verschlüsselung ist das berühmteste polyalphabetische Verschlüsselungsverfahren und wurde im Jahr 1586 von dem französischen Diplomaten Blaise de Vigenère (1523 - 1596) veröffentlicht. Die Stärke der Vigenère-Verschlüsslung besteht darin, dass bis zu 26 verschiedene Geheimtextalphabete benutzt werden, um eine Nachricht zu verschlüsseln. Dazu benötigt man ein sogenanntes Vigenère-Quadrat und ein beliebiges, zwischen dem Sender und dem Empfänger vereinbartes, Schlüsselwort. Im Vigenère-Quadrat sind unter einem Klartextalphabet alle 26 Geheimtextalphabete aufgelistet, jeweils um einen Buchstaben gegenüber dem vorhergehenden Alphabet nach links verschoben (vgl. Tabelle 4). Die Buchstaben des Schlüsselworts geben an, mit welchem Geheimtextalphabet bestimmte Klartextbuchstaben verschlüsselt werden.

[16] Vgl. Beutelspacher (2002), S. 29 und Freiermuth et al. (2010), S. 93

Schlüssel	Klartext: 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
0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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

Tabelle 4: Ein Vigenère-Quadrat[17]

[17] Vgl. Singh (2002), S. 68

Möchten wir zum Beispiel den Klartext „Vigenère-Chiffre“ anhand des Schlüsselworts „GEHEIM“ verschlüsseln, schreiben wir zunächst das Schlüsselwort über die Nachricht und zwar so lange, bis die Länge des Klartextes erreicht ist:

```
Schlüssel   G E H E I M G E H E I M G E H
Klartext    v i g e n e r e c h i f f r e
Geheimtext  B M N I V Q X I J L Q R L V L
```

Der Buchstabe des Schlüsselworts bestimmt nun, mit welchem Geheimtextalphabet, also mit welcher Zeile des Vigenère-Quadrats, der darunter stehende Klartextbuchstabe verschlüsselt wird. Um den ersten Buchstaben `v` zu verschlüsseln, müssen wir die Zeile des Vigenère-Quadrats verwenden, welche mit `G` beginnt. In dieser Zeile sehen wir nach, was in der Spalte `v` steht. Dort steht der Buchstabe `B`, also wird der Klartextbuchstabe `v` durch den Buchstaben `B` verschlüsselt. Für den zweiten Buchstaben `i` suchen wir den Buchstaben in der Zeile `E` und der Spalte `i`, das ist der Buchstabe `M`, usw. Zum Entschlüsseln eines Geheimtextbuchstaben bestimmen wir mit dem darüber stehenden Schlüsselbuchstaben das Geheimtextalphabet, suchen in diesem Alphabet den Geheimtextbuchstaben und gehen zu dem darüber liegenden Klartextbuchstaben.

Schon an unserem kleinen Beispiel kann man erkennen, dass die Häufigkeit der Buchstaben gleichmäßiger verteilt ist, als bei einer monoalphabetischen Verschlüsselung. Ein Kryptoanalytiker, der die Häufigkeitsanalyse auf diesen Geheimtext anwendet, wird annehmen, dass der häufigste Geheimtextbuchstabe `L`, dem im Deutschen häufigsten Buchstaben `e` entspricht. Der Geheimtextbuchstabe `L` steht aber für drei verschiedene Klartextbuchstaben `h`, `f` und `e`. Umgekehrt kommt das `f` im Klartext doppelt vor und wird mit zwei verschiedenen Buchstaben `R` und `L` verschlüsselt.

Mit dem Vigenère-Quadrat ist es aber relativ mühsam, einen längeren Text zu verschlüsseln. Um nicht immer die gesamte Tabelle zu benutzen, kann man bei einem bestimmten Schlüsselwort nur die Zeilen des Geheimtextalphabets notieren, deren erste Buchstaben das Schlüsselwort ergeben. Dieser Ausschnitt des Vigenère-Quadrats lässt sich leichter benutzen[18]. Für das Beispiel zuvor erhält man folgende Zeilen:

[18] Vgl. Karpfinger und Kiechle (2010), S. 12

	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
4	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
6	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
7	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
8	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
12	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

Zur Beschleunigung der Verschlüsselung kann auch eine sogenannte *Chiffrierscheibe* oder *Alberti-Scheibe* (vgl. Abbildung 3) verwendet werden. Die Chiffrierscheibe ist die erste kryptografische „Maschine", die das Verschlüsseln mechanisiert und wurde bereits 1470 von dem italienischen Architekten Leon Battista Alberti (1404 - 1472) erfunden. Sie besteht aus zwei unterschiedlich großen, runden Scheiben, auf deren Ränder jeweils das Alphabet in natürlicher Reihenfolge geschrieben ist. Die kleinere Scheibe wird auf die größere gelegt und sie werden an ihren Mittelpunkten so aneinander befestigt, dass die innere Scheibe gedreht werden kann. Damit kann man die gewünschte Verschiebung einstellen. Auf der äußeren Scheibe befindet sich das Klartextalphabet und auf der inneren das Geheimtextalphabet.

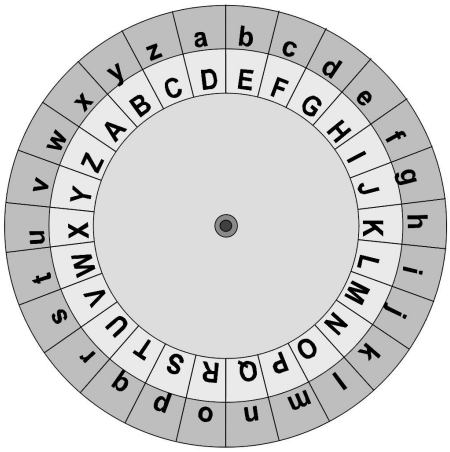


Abbildung 3: Eine Chiffrierscheibe[19]

Wird die Einstellung der Scheibe wie in Abbildung 3 gewählt, wird zum Beispiel der Klartextbuchstabe `a` mit dem Geheimtextbuchstaben `D` verschlüsselt. Bleibt diese Einstellung während der Verschlüsselung einer Nachricht unverändert, erhält man eine einfache monoalphabetische Verschlüsselung, nämlich die Caesar-Verschiebung um drei Stellen. Ändert man die Einstellung der Scheibe während der Verschlüsselung, bekommt man die

[19] Beutelspacher (2009), S. 7

Vigenère-Verschlüsselung, also eine polyalphabetische Verschlüsselung.

Die Vigenère-Verschlüsselung kann ähnlich wie bei der Caesar-Verschiebung durch die Ver- und Entschlüsselungsfunktion

$$V(x) = x + k_i \bmod n \text{ und } E(c) = c - k_i \bmod n \text{ für } i = 1, \ldots, d$$

auf der Menge $\mathbb{Z}_n$ beschrieben werden, wenn einem Alphabet mit n Buchstaben, die Zahlen 0 bis $n-1$ zugeordnet werden. Der Schlüssel k besteht diesmal aber nicht aus einer einzigen Zahl, sondern einer Folge von Zahlen $k_1 k_2 \ldots k_d$, wobei d die Länge des Schlüsselworts und k_i die Zahl des i-ten Schlüsselwortbuchstabens ist.

Im folgenden Beispiel wird gezeigt, wie der Geheimtext „QIFOMKORYMLPSGFD", welcher mit dem Schlüsselwort „KEY" erzeugt wurde, in $\mathbb{Z}_{26}$ entschlüsselt wird.

Schlüssel	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K
Geheimtext	Q	I	F	O	M	K	O	R	Y	M	L	P	S	G	F	D
Geheimtext in Zahlen	16	8	5	14	12	10	14	17	24	12	11	15	18	6	5	3
- Schlüssel in Zahlen	10	4	24	10	4	24	10	4	24	10	4	24	10	4	24	10
Differenz	6	4	-19	4	8	-14	4	13	0	2	7	-9	8	2	-19	-7
modulo 26	6	4	7	4	8	12	4	13	0	2	7	17	8	2	7	19
Klartext	g	e	h	e	i	m	e	n	a	c	h	r	i	c	h	t

Die Häufigkeit der Buchstaben ist bei einer Vigenère-Verschlüsselung gleichmäßiger verteilt, als bei einer monoalphabetischen Verschlüsselung, deswegen lässt sich diese, wie bereits erwähnt, mittels Häufigkeitsanalyse nicht brechen. Auch eine systematische Schlüsselsuche würde nicht zum Erfolg führen. Die Anzahl der möglichen Schlüssel ist enorm, da jedes Wort, beliebige selbst erfundene Wörter oder auch ganze Sätze als Schlüssel verwendet werden können. Dieses Verfahren galt über 300 Jahre als unknackbar, bis der preußische Offizier Friedrich Wilhelm Kasiski (1805 - 1881) im Jahr 1863 eine Methode veröffentlichte, die es ermöglicht, die Vigenère-Verschlüsselung zu brechen. Das Ziel dieser Methode ist, die Schlüsselwortlänge zu bestimmen.

Angenommen, wir wissen, dass das Schlüsselwort aus n Buchstaben besteht. Dann werden die Klartextbuchstaben an den Stellen 1, $n+1$, $2n+1$, ... mit dem Geheimtextal-

phabet verschlüsselt, das mit dem ersten Buchstaben des Schlüsselworts beginnt. Die Buchstaben an den Stellen 2, n+2, 2n+2, ... werden mit dem zweiten Schlüsselwortbuchstaben verschlüsselt, usw. Teilen wir nun die Buchstaben des Geheimtextes in n Gruppen auf, die mit dem gleichen Schlüsselwortbuchstaben verschlüsselt wurden, erhalten wir jeweils einen Teil des Geheimtextes, welches durch eine Caesar-Verschiebung entstanden ist. Anschließend bestimmen wir für jede Gruppe separat den häufigsten Buchstaben. Handelt es sich um einen deutschen Text, wird dieser Buchstabe höchstwahrscheinlich dem `e` entsprechen. Wir bestimmen das entsprechende Geheimtextalphabet, indem wir in der Spalte `e`, den häufigsten Buchstaben dieser Gruppe finden. Der erste Buchstabe dieser Zeile ist dann der entsprechende Schlüsselwortbuchstabe. Auf diese Weise können wir Schritt für Schritt das gesamte Schlüsselwort bestimmen, vorausgesetzt wir wissen, wie viele Buchstaben das Schlüsselwort hat.[20]

Kasiski-Test

Die Methode zur Bestimmung der Schlüsselwortlänge wurde bereits 1854 vom englischen Mathematiker Charles Babbage (1792 - 1871), der vor allem für den ersten Entwurf eines modernen Computers bekannt ist, entwickelt. Er hat seine Entdeckung aber nie veröffentlicht. Neun Jahre später wurde das Verfahren auch von Kasiski entdeckt. Da er es veröffentlichte, wird diese Methode als Kasiski-Test bezeichnet.

Im Allgemeinen werden gleiche Buchstabenfolgen im Klartext mit unterschiedlichen Geheimtextfolgen verschlüsselt:

```
Schlüssel   G E H E I M G E H E I M G E H E I M G E H
Klartext    . . e i n . . . . . e i n . . . . e i n .
Geheimtext  . . L M V . . . . . M U T . . . . Q O R .
```

Doch Babagge und Kasiski bemerkten, dass Buchstabenfolgen im Geheimtext wiederholt auftraten. Solche Wiederholungen entstehen meistens dann, wenn dieselben Buchstabenfolgen im Klartext mit demselben Teil des Schlüsselworts verschlüsselt werden:

[20] Vgl. Beutelspacher (2002), S. 32

```
Schlüssel   G E H E I M G E H E I M G E H E I M G E H
Klartext    e i n . . . e i n . . . . . . . . . e i n
Geheimtext  L M V . . . L M V . . . . . . . . . L M V
```

Das ist genau dann der Fall, wenn der Abstand zwischen den beiden Klartextfolgen ein Vielfaches der Schlüsselwortlänge ist, wobei der Abstand die Anzahl der Buchstaben ist, um die die zweite Folge gegenüber der ersten verschoben ist. In unserem Beispiel ist das zweite `ein` um sechs Buchstaben gegenüber dem ersten `ein` verschoben und das dritte um 18 bzw. zwölf Buchstaben gegenüber dem ersten bzw. zweiten `ein`. Wenn die Buchstaben des Klar- bzw. Geheimtextes durchnummeriert werden, ist der Abstand die Differenz der beiden Positionen, auf der die gleichen Buchstabenfolgen vorkommen[21]. Das `ein` kommt in unserem Beispiel an den Positionen 1, 7 und 19 vor. Bestimmen wir die Differenzen zwischen je zwei Positionen, so erhalten wir die gleichen Abstände wie zuvor.

Hat man nun mehrere sich wiederholende Buchstabenfolgen im Geheimtext gefunden, bestimmt man deren Abstände. Im Allgemeinen ist die Schlüsselwortlänge ein Teiler dieser Abstände, also ist die Länge des Schlüsselworts ein Teiler vom größten gemeinsamen Teiler aller Abstände.

Wiederholungen von Buchstabenfolgen im Geheimtext können jedoch auch zufällig entstehen. Diese kann man erkennen, da sie meistens Abstände liefern, die zu den meisten Abständen teilerfremd sind[22]. Solche Ausreißer muss man bei der Berechnung ausschließen. Betrachtet man zusätzlich längere Buchstabenfolgen, die mindestens aus vier Buchstaben bestehen, dann ist die Wiederholung von zufällig entstandenen gleichen Folgen sehr unwahrscheinlich.

Wir betrachten nun den folgenden Geheimtext:

```
VIFYJZTHKZ KMYCVJBQOL FBAOJZBAAY VIMAKWVXRH JBRDAAVQKU YMUKPEBRDA
MUMADSVQKS FIHIOVMEKT HNNKUYMEHY SCPNAWAHSK WVTKOWQZZL PBJOLVMEOU
VMAQSSZGKE LHHALTMEYL LHRTDWVACP JIYYVVIFYJ ZTHKZKMYCV JBNAZXQAJP
YUNIOWVXUL FVGKUOIRXL WAROUDMVIO LMFJLFBRDA RCRTARQSLL JV
```

[21] Vgl. Freiermuth et al. (2010), S. 100
[22] Vgl. Karpfinger und Kiechle (2010), S. 13

Wir wissen, dass es sich um einen deutschen Text handelt, der mit dem Vigenère-Verfahren verschlüsselt wurde und möchten den zugehörigen Klartext ermitteln. Um die Schlüsselwortlänge zu bestimmen, wenden wir zuerst den Kasiski-Test an. Dazu suchen wir Buchstabenfolgen, aus mindestens vier Buchstaben, die wiederholt auftreten und bestimmen deren Abstände:

```
VIFYJZTHKZ KMYCVJBQOL FBAOJZBAAY VIMAKWVXRH JBRDAAVQKU YMUKPEBRDA
MUMADSVQKS FIHIOVMEKT HNNKUYMEHY SCPNAWAHSK WVTKOWQZZL PBJOLVMEOU
VMAQSSZGKE LHHALTMEYL LHRTDWVACP JIYYVVIFYJ ZTHKZKMYCV JBNAZXQAJP
YUNIOWVXUL FVGKUOIRXL WAROUDMVIO LMFJLFBRDA RCRTARQSLL JV
```

Buchstabenfolge	Abstand
VIFYJZTHKZKMYCVJB	155
KUYM	35
BRDA	15, 160 und 175

Die Länge des Schlüssels wird wahrscheinlich ein gemeinsamer Teiler dieser Abstände sein. Als Schlüsselwortlänge kommen der größte gemeinsame Teiler und alle seine Teiler in Frage. Der größte gemeinsame Teiler der Abstände ist $ggT(15, 35, 155, 160, 175) = 5$. Da 5 keine weiteren Teiler hat, können wir annehmen, dass das Schlüsselwort die Länge 5 hat.

Im nächsten Schritt suchen wir das Schlüsselwort selbst mit fünf Buchstaben. Dazu unterteilen wir den Geheimtext in fünf Teiltexte. Alle Geheimtextbuchstaben, die mit dem ersten Schlüsselwortbuchstaben verschlüsselt wurden, werden dem ersten Teiltext zugeordnet, das ist der 1., 6., 11., ... Buchstabe im Geheimtext. Dem zweiten Teiltext wird der 2., 7., 12., ... Buchstabe zugeordnet, usw.

1. Teiltext: VZKJFZVWJAYEMSFVHYSWWWPVVSLTLWJVZKJXYWFOWDLFRRJ
2. Teiltext: ITMBBBIVBVMBUVIMNMCAVQBMMZHMHVIITMBQUVVIAMMBCQV
3. Teiltext: FHYQAAMXRQURMQHENEPHTZJEAGHERAYFHYNANXGRRVFRRS
4. Teiltext: YKCOOAARDKKDAKIKKHNSKZOOQKAYTCYYKCAJIUKXOIJDTL
5. Teiltext: JZVLJYKHAUPADSOTUYAKOLLUSELLDPVJZVZPOLULUOLAAL

Von diesen Teiltexten wird nun der Buchstabe bestimmt, der am häufigsten auftritt. Da es sich um einen deutschen Text handelt, wird der jeweilige Buchstabe höchstwahrscheinlich dem e entsprechen. Damit bestimmen wir die jeweiligen Geheimtextalphabete und erhalten das Schlüsselwort.

Teiltext	Häufigster Buchstabe	Schlüsselwortbuchstabe
1.	W → e	S
2.	M → e	I
3.	R → e	N
4.	K → e	G
5.	L → e	H

Das Schlüsselwort lautet also SINGH. Nun können wir den Geheimtext leicht entschlüsseln. Es entsteht ein Text, der Sinn ergibt:

> dasschlues selwortdie ntnichtnur dazudenkla rtextinden geheimtext
> umzuwandel nauchderem pfaengerbr auchtesumd engeheimte xtwiederin
> denklartex tzuueberse tzenwennwi ralsodassc hluesselwo rtausfindi
> gmachenkoe nntenwaere eseinleich tesdentext zuentziffe rn

Fügen wir sinnvolle Wortzwischenräume und Satzzeichen ein, dann erhalten wir:

> „Das Schlüsselwort dient nicht nur dazu, den Klartext in den Geheimtext zu verwandeln, auch der Empfänger braucht es, um den Geheimtext wieder in den Klartext zu übersetzen. Wenn wir also das Schlüsselwort ausfindig machen können, wäre es ein leichtes, den Text zu entziffern.“[23]

Würde sich hier kein sinnvoller Text ergeben, müssten wir unsere Annahmen ändern. Eine Möglichkeit wäre, es mit einem anderen Kandidaten für die Schlüsselwortlänge zu versuchen, falls mehrere in Frage kommen. Eine andere Möglichkeit ist, falls die Häufigkeit der Buchstaben in den Teiltexten sehr nah aneinander liegen, den häufigsten

[23] Singh (2002), S. 80

Buchstaben durch den zweithäufigsten zu ersetzen. Oder man ersetzt den häufigsten Buchstaben im Teiltext durch den zweithäufigsten Buchstaben der jeweiligen Sprache.

Wir konnten diesen Text deshalb so einfach knacken, da das Schlüsselwort, im Vergleich zum Geheimtext, sehr kurz ist. Je länger das Schlüsselwort gewählt wird, desto schwieriger lässt sich der Geheimtext brechen.

Enigma

Da somit auch die Vigenère-Verschlüsselung geknackt wurde, mussten neue, sichere Verschlüsselungsverfahren entwickelt werden. Es wurden die ersten kryptographischen Maschinen gebaut. Die bekannteste Verschlüsselungsmaschine dieser Zeit, die vom deutschen Ingenieur Arthur Scherbius (1878 - 1929) entwickelt und 1918 zum Patent angemeldet wurde, ist die Enigma. Sie wurde vor allem vom deutschen Militär nach dem Ersten Weltkrieg und während des Zweiten Weltkriegs eingesetzt. Im Grunde ist sie eine verbesserte, elektrische Version der Alberti-Scheibe.

Die Enigma sieht wie eine altmodische Schreibmaschine aus und besteht in ihrer Grundausführung aus drei Bestandteilen: einer Tastatur, einer Verschlüsselungseinheit, die im Gehäuse verborgen ist, und einem Lampenfeld (vgl. Abbildung 4).

Abbildung 4: Eine Enigma der Wehrmacht[24]

[23]Borys (2011), S. 152

Zum Verschlüsseln einer Nachricht werden die Klartextbuchstaben über die Tastatur eingegeben. Durch die Eingabe werden elektrische Signale ausgelöst, die durch die Verschlüsselungseinheit fließen und die Lampe für den entsprechenden Geheimtextbuchstaben zum Leuchten bringen.

Der wichtigste Teil der Verschlüsselungseinheit ist eine Scheibe die von Drähten durchzogen ist und Walze oder Rotor genannt wird. Die Verschlüsselung der Klartextbuchstaben wird durch die Verdrahtung im Inneren der Walze bestimmt.

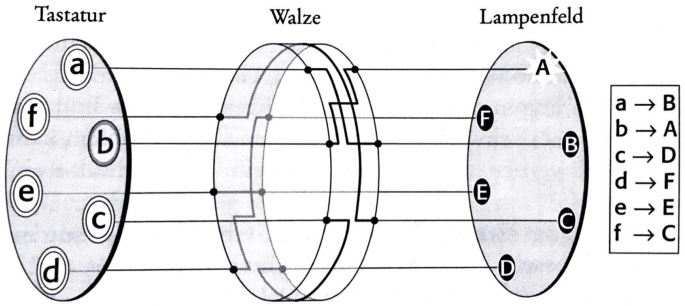


Abbildung 5: Eine vereinfachte Version der Enigma mit einem aus nur sechs Buchstaben bestehenden Alphabet.[25]

In Abbildung 5 leuchtet zum Beispiel durch die Eingabe des Klartextbuchstaben `b` der Geheimtextbuchstabe `A` auf. In dieser Einstellung legt die Walze ein Geheimtextalphabet fest und kann eine einfache monoalphabetische Verschlüsselung erzeugen. Nach jeder Eingabe eines Buchstaben dreht sich die Walze allerdings automatisch um eine Position weiter. Das entspricht, bei einem Alphabet mit 26 Buchstaben, einer Drehung um ein Sechsundzwanzigstel ihres Umlaufs. Damit ändert sich nach jeder Eingabe das Geheimtextalphabet und es wird eine polyalphabetische Verschlüsselung mit 26 verschiedenen Geheimtextalphabeten erzeugt. Nachdem 26 Buchstaben eingegeben werden, kehrt die Walze in ihre Ausgangsposition oder Grundstellung zurück und das Verschlüsselungsmuster wiederholt sich. Die Grundstellung der Walze ist der Schlüssel und da die Walze 26 verschiedene Positionen annehmen kann, gibt es 26 mögliche Schlüssel, mit der eine Nachricht verschlüsselt werden kann.

Die Anzahl der Schlüssel kann erhöht werden, wenn eine zweite Walze eingebaut wird. Die zweite Walze dreht sich erst dann um eine Position, wenn die erste Walze eine vollständige Umdrehung abgeschlossen hat. Das Verschlüsselungsmuster wiederholt sich,

[25] Singh (2002), S. 126

wenn die zweite Walze wieder in ihrer Ausgangsposition ist. Daraus ergeben sich $26 \cdot 26 = 676$ unterschiedliche Walzenstellungen und somit 676 mögliche Schlüssel.

Im Grundmodell der Enigma wurde eine dritte Walze und ein Reflektor oder eine Umkehrwalze eingebaut (vgl. Abbildung 6).

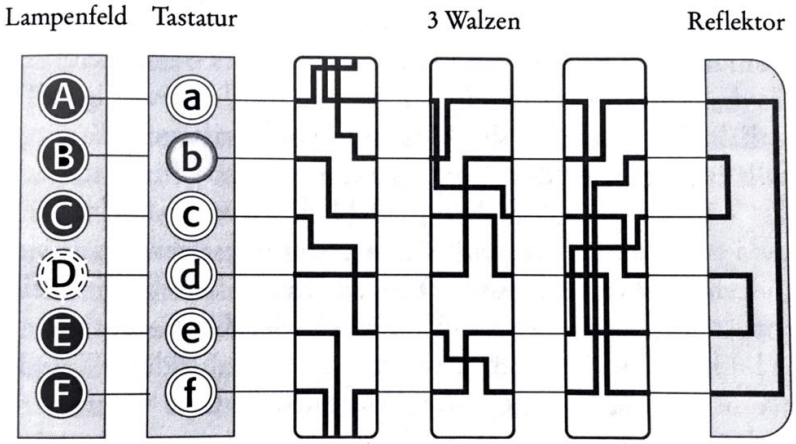


Abbildung 6: Grundmodell der Enigma[26]

Der Reflektor ähnelt einer Walze, doch er hat nur Kontakte auf einer Seite und rotiert nicht. Wird ein Buchstabe eingetippt, gelangt ein elektrisches Signal durch die drei Walzen zum Reflektor. Dieser schickt das Signal über einen anderen Weg durch die Walzen zurück und es leuchtet der entsprechende Geheimtextbuchstabe auf. In Abbildung 6 wird zum Beispiel der Buchstabe `b` eingegeben und der Buchstabe `D` leuchtet auf. Wenn das Signal durch den Reflektor wieder zurückgeschickt wird, wird es aber nicht wie es in der Abbildung scheint, wieder durch die Tastatur, sondern direkt auf das Lampenfeld geleitet. Der Reflektor erhöht zwar nicht die Anzahl der Geheimtextalphabete, doch dieser bewirkt eine einfache Entschlüsselung. Wird die Maschine in dieselbe Einstellung gebracht, wie beim Verschlüsseln, leuchtet nach dem Eintippen des Geheimtextbuchstaben der zugehörige Klartextbuchstabe auf. Also benötigen Sender und Empfänger eine Enigma mit der gleichen Grundstellung.

Um die Anzahl der möglichen Grundeinstellungen und somit der Schlüssel zu erhöhen, nahm Scherbius zwei Veränderungen an der Enigma vor. Die Reihenfolge der Walzen konnten vertauscht werden. Also gab es $3! = 6$ Möglichkeiten, die Walzen neu anzuord-

[26] Singh (2002), S. 131

nen[27]. Des Weiteren wurde ein Steckerbrett zwischen der Tastatur und der ersten Walze eingebaut. Das Steckerbrett ermöglichte über eine Kabelverbindung das Vertauschen von zwei Buchstaben, bevor das Signal in die Walze eintrat (vlg. Abbildung 7). Es wurden 6 Kabel verwendet, womit bis zu sechs Buchstabenpaare vertauscht werden konnten.

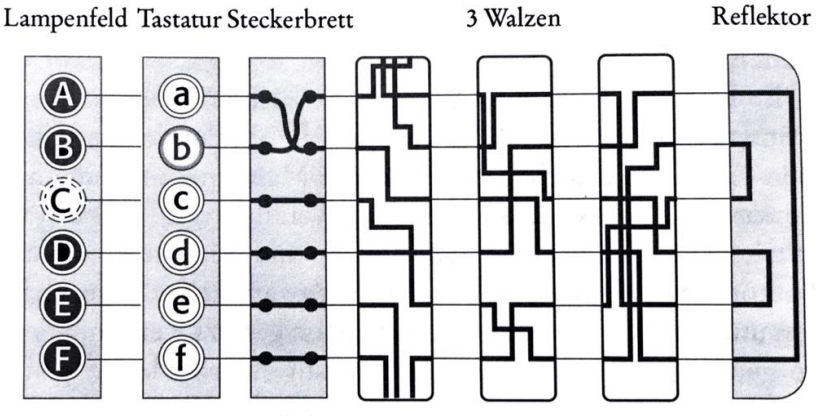


Abbildung 7: Grundmodell der Enigma mit Steckerbrett[28]

Die vertauschten Buchstaben gehören mit zur Grundeinstellung der Maschine und müssen zwischen Sender und Empfänger zuvor vereinbart werden. Die Anzahl der möglichen Schlüssel für eine Enigma mit drei Walzen und einem Steckerbrett mit 6 Kabel lässt sich wie folgt berechnen:

Walzenstellungen:
Jede der drei Walzen kann auf 26 verschiedene Stellungen gebracht werden. Somit gibt es $26 \cdot 26 \cdot 26$ mögliche Einstellungen. 17.576

Walzenlagen:
Die drei Walzen können in $3! = 6$ verschiedene Reihenfolgen gebracht werden. 6

Steckerbrett:
Bei 26 Buchstaben sind bis zu 13 Vertauschungen möglich. Für eine Vertauschung gibt es $\binom{26}{2}$ Steckmöglichkeiten. Das ist die Anzahl der Möglichkeiten, zwei Buchstaben aus 26 auszuwählen[29]. Für die zweite Verbindung stehen nur noch 24 Buchstaben

[27] Vgl. Satz 1
[28] Singh (2002), S. 134
[29] Vgl. Binomialkoeffizient, S. 7

zur Verfügung und es ergeben sich $\binom{24}{2}$ mögliche Steckverbindungen. Für 6 Kabel stehen $\binom{26}{2} \cdot \binom{24}{2} \cdot \binom{22}{2} \cdot \binom{20}{2} \cdot \binom{18}{2} \cdot \binom{16}{2}$ Möglichkeiten zur Verfügung. Da die Reihenfolge der Steckverbindungen keine Rolle spielt und es 6! Anordnungsmöglichkeiten gibt, muss noch durch 6! dividiert werden:

$$\frac{\binom{26}{2} \cdot \binom{24}{2} \cdot \binom{22}{2} \cdot \binom{20}{2} \cdot \binom{18}{2} \cdot \binom{16}{2}}{6!} = \frac{\frac{26!}{24! \cdot 2!} \cdot \frac{24!}{22! \cdot 2!} \cdots \frac{16!}{14! \cdot 2!}}{6!} = \\ = \frac{\frac{26!}{14! \cdot 2^6}}{6!} = \frac{26!}{14! \cdot 2^6 \cdot 6!} \qquad 100.391.791.500$$

Die mögliche Anzahl der Steckverbindungen mit n Kabel aus einem Alphabet mit N Buchstaben lässt sich mit folgender Formel berechnen:

$$\frac{N!}{(N-2n)! \cdot 2^n \cdot n!}$$

Gesamtzahl:
Wenn die drei Zahlen miteinander multipliziert werden, erhält man die Gesamtanzahl der möglichen Schlüssel. 10.586.916.764.424.000

Mit dieser großen Anzahl an mögliche Schlüsseln und der Komplexität der Enigma, galt sie als unknackbar.

Ab 1926 wurde die Enigma vom Deutschen Militär zur Übermittlung von Funksprüchen eingesetzt. Die Grundstellung, bestehend aus den Steckverbindungen am Steckerbrett, der Reihenfolge der Walzen und den Walzenstellungen, wurden in einem Schlüsselbuch aufgelistet und an alle Chiffreure im Funknetz verteilt. Jeden Tag wurde ein neuer Schlüssel verwendet. Bei längeren Texten, die mit dem gleichen Schlüssel verschlüsselt sind, ist es im Allgemeinen leichter diese zu brechen, deswegen legten die Deutschen zusätzlich für jede Meldung einen neuen Spruchschlüssel fest. Der Spruchschlüssel ist eine selbstgewählte Walzenstellung, die mittels Tagesschlüssel vor der eigentlichen Nachricht übermittelt wurde. Das System schien undurchdringlich, doch den Polen gelang es bereits 1932 die Enigma vollständig zu analysieren. Marian Rejewski entwickelte eine Technik, mit der er den Tagesschlüssel finden und damit den Geheimtext entschlüsseln konnte. Zusätzlich erfand er eine Maschine, die alle möglichen Walzenstellungen überprüfte, bis sie die richtige Einstellung fand. Bei sechs möglichen Walzenlagen mussten sechs Maschinen parallel arbeiten. Die Anlage wurde als *Bombe* bezeichnet und benötigte etwa

zwei Stunden um den Tagesschlüssel zu finden.

Obwohl die Deutschen nicht wussten, dass die Enigma geknackt worden war, nahmen sie immer wieder Verbesserungen am System vor. Ende 1938 wurden zwei weitere Walzen eingeführt. Damit setzte sich die Walzenlage aus drei von fünf möglichen Walzen zusammen. Für die erste Position der Walzen konnte eine von fünf Walzen, für die zweite Position eine von vier Walzen und für die dritte Position eine von drei Walzen ausgewählt werden. Die Anzahl der möglichen Walzenlagen stieg von 6 auf $5 \cdot 4 \cdot 3 = 60$. Zusätzlich wurde die Zahl der Steckerkabel von 6 auf 10 erweitert. Die Anzahl der möglichen Schlüssel stieg auf

$$17.576 \cdot 60 \cdot \frac{26!}{(26-20)! \cdot 2^{10} \cdot 10!} = 158.962.555.217.826.360.000.$$

Die Polen waren nicht mehr in der Lage, den Tagesschlüssel zu bestimmen, weil der Aufwand zu groß wurde und sie die erforderlichen technischen Mittel nicht hatten. Sie teilten ihre Erkenntnisse mit französischen und britischen Kryptoanalytikern. Im Entschlüsselungszentrum der Engländer wurde es schließlich dank dem Mathematiker Alan Turing (1912 - 1954) möglich, die Enigma zu knacken. Er entwickelte zudem eine Maschine, die ebenfalls als *Bombe* bezeichnet wurde, um die Walzeneinstellungen der Enigma zu überprüfen. Somit konnten die Engländer die verschlüsselten Geheimbotschaften der deutschen Wehrmacht ab 1940 unbemerkt entschlüsseln[30]. Bei der Entwicklung und Verfeinerung der Analyse der Enigma, wurde auf Grundlage von Alan Turings Konzept, der erste digitale und programmierbare Computer, der *Colossus*, gebaut und ab Ende 1943 eingesetzt. Die Entschlüsselung der Enigma soll den Zweiten Weltkrieg wesentlich verkürzt haben.

Die Funktionsweise und die Anzahl möglicher Schlüssel der Enigma soll zeigen, dass auch ein kompliziertes Verfahren mit einer gigantischen Anzahl an möglichen Schlüssel gebrochen werden kann.[31]

[30] Vgl. Beutelspacher (2002), S. 35

[31] Welche Faktoren bei der Entschlüsselung der Enigma entscheidend waren und mit welchen Methoden sie entschlüsselt wurde, kann zum Beispiel in Singh (2002), S. 137-174 nachgelesen werden.

One-Time-Pad

Damit die Deutschen bis Kriegsende nicht wussten, dass die Enigma geknackt worden war, benutzte die englische Entschlüsselungstruppe ein anderes Verfahren, das One-Time-Pad, um die entschlüsselten Nachrichten der Deutschen, an den Premierminister zu übermitteln.

Das Verfahren funktioniert genau so, wie die Vigenère-Verschlüsselung, der Schlüssel ist aber gleich lang, wie die zu verschlüsselnde Nachricht, besteht aus einer zufälligen Buchstabenfolge und wird nur einmal verwendet. Die Schlüsselbuchstaben wurden auf die Blätter eines Abreißblocks geschrieben. Wenn ein Schlüsselbuchstabe verwendet wurde, wurde das Blatt abgerissen und weggeschmissen, daher der Name *One-Time-Pad* („Einmalblock").

Bei den Verschlüsselungsverfahren, die bis jetzt besprochen wurden, erkennt man, dass man sie gebrochen hat, weil der Geheimtext mit dem richtigen Schlüssel einen sinnvollen, mit dem falschen Schlüssel hingegen einen sinnlosen Text ergibt[32]. Beim One-Time-Pad kann ein Geheimtext aber zu jedem Klartext entschlüsselt werden. Das heißt, dass es zu jedem Klartext und zu jedem Geheimtext, einer bestimmten Länge, genau einen Schlüssel gibt, der den Geheimtext in den Klartext übersetzt.

Verschlüsseln wir zum Beispiel die Nachricht „Dieser Satz ist geheim." mit einer zufälligen Buchstabenfolge, erhalten wir folgenden Geheimtext[33]:

```
Schlüssel   Q X V H C A M D M Z S J E C B Y D P M
Klartext    d i e s e r s a t z i s t g e h e i m
Geheimtext  T F Z Z G R E D F Y A B X I F F H X Y
```

Wenn ein Angreifer diesen Geheimtext abfängt und nicht weiß, welcher Schlüssel verwendet wurde, kann er jeden möglichen Klartext, der aus 19 Buchstaben besteht, herausbekommen, wie zum Beispiel:

[32] Vgl. Schwenk (2014), S. 12
[33] Das Beispiel stammt aus Beutelspacher (2002), S. 38f. und wurde erweitert.

```
Schlüssel   H F G S C F E B Y F F T M X N Q H F G
Klartext    m a t h e m a c h t v i e l s p a s s
Geheimtext  T F Z Z G R E D F Y A B X I F F H X Y

Schlüssel   P X M F T H R D D O Z B G E O M D A F
Klartext    e i n u n k n a c k b a r e r t e x t
Geheimtext  T F Z Z G R E D F Y A B X I F F H X Y
```

Ein Angreifer kann nicht sagen, welcher Klartext der richtige ist, er kann nur raten. Es lohnt sich daher nicht, jede mögliche Kombination aus Schlüsselbuchstaben zu überprüfen.

Ein Geheimtext, der mit dem One-Time-Pad verschlüsselt wurde, ist unknackbar. Wichtig ist hierbei, dass die Buchstabenfolge für den Schlüssel, der die gleiche Länge hat wie der Klartext, rein zufällig gewählt und nur einmal verwendet wird. Verwendet man als Schlüssel zum Beispiel einen Text aus einem Buch, hat es den Vorteil, dass dieser zwischen Sender und Empfänger leicht übermittelt werden kann. Man könnte auch die Schlüsselwortlänge nicht bestimmen, da der Schlüssel gleich lang ist, wie der Klartext. Weil der Schlüssel aber zum Beispiel ein deutschsprachiger Text ist, lassen sich durch statisch erfassbare Daten mögliche Ansatzpunkte für eine Kryptoanalyse finden. Wird eine Schlüsselfolge ein zweites Mal verwendet, kann ein Angreifer verschiedene Schlüsselfolgen ausprobieren. Lassen sich mit einer Schlüsselfolge beide Geheimtexte jeweils zu sinnvollen Texten entschlüsseln, hat er die Schlüsselfolge gefunden[34].

Da heute zum Verschlüsseln Computer verwendet werden, wird das One-Time-Pad nicht mit Buchstaben, sondern mit Bits, das sind Elemente der Menge $\mathbb{Z}_2 = \{0, 1\}$, betrieben. Die Klartext- und die Schlüsselbuchstaben werden als Bitfolge dargestellt. Die Verschlüsselung erfolgt durch bitweise Addition modulo 2:

```
Schlüssel   1 1 0 0 1 0 1 1 1 0 0
Klartext    1 0 1 0 1 0 1 0 1 0 1
Geheimtext  0 1 1 0 0 0 0 1 0 0 1
```

Das entspricht einer bitweise XOR-Operation ($\oplus$, *exclusive or*):

[34] Vgl. Freiermuth et al. (2010), S. 141

$$0 \oplus 0 = 0,\ 1 \oplus 0 = 1,\ 0 \oplus 1 = 1,\ 1 \oplus 1 = 0$$

Da Addition und Subtraktion modulo 2 identisch sind, kann mit derselben Operation auch entschlüsselt werden (vgl. Abbildung 8).

Abbildung 8: Vernam-Chiffre: Bitweise Ver- und Entschlüsselung einer Nachricht[35]

Die bitweise Verschlüsselung mit dem One-Time-Pad wurde 1917 von dem amerikanischen Ingenieur Gilbert S. Vernam (1890 - 1960) erfunden, daher wird das One-Time-Pad auch als Vernam-Chiffre bezeichnet[36].

Obwohl das Verfahren nicht gebrochen werden kann, wird es in der Praxis sehr selten benutzt. Abgesehen davon, dass man für jede Nachricht einen zufälligen Einmalschlüssel erzeugen muss, ist der Schlüsselaustausch sehr aufwändig. Sender und Empfänger müssen für jede Nachricht, die sie übermitteln möchten, zuvor einen gleich langen Schlüssel auf sicherem Weg ausgetauscht haben.

2.1.3 Problem der Schlüsselverteilung

Bei der symmetrischen Verschlüsselung verwenden Sender und Empfänger, zum Ver- und Entschlüsseln einer Nachricht, den gleichen Schlüssel. Das bedeutet, dass ein geheimer Schlüssel ausgetauscht werden muss, bevor eine Kommunikation stattfinden kann. Das Problem besteht nun darin, den Schlüssel sicher zu übertragen. Würde man den Schlüssel verschlüsselt übertragen, dann bräuchte der Empfänger einen weiteren Schlüssel, um diesen zu entschlüsseln. Erfolgt die Übertragung als Klartext, kann ein Angreifer

[35] Spitz et al. (2011), S. 11
[36] Vgl. Spitz et al. (2011) S. 10

den Schlüssel abfangen und die eigentliche Nachricht damit entschlüsseln. Die sicherste Möglichkeit ist die persönliche Übergabe des Schlüssels, was sehr zeitaufwändig ist. Eine weitere Möglichkeit, welche weniger sicher und teurer ist, besteht darin, den Schlüssel von einem Boten überbringen zu lassen. Auf diese Art übermittelten früher zum Beispiel die Banken ihren Kunden die Schlüssel. Doch es wurden immer mehr Daten verschickt und immer mehr Schlüssel mussten verteilt werden. Die Schlüsselverteilung wurde zu einem großen Problem. Es gab Kryptologen, die behaupteten, dass dieses Problem unlösbar sei. Ab Mitte der siebziger Jahre wurden neue Verfahren, die asymmetrischen Verschlüsslungen, entwickelt, mit denen das Problem der Schlüsselverteilung gelöst wurde.

2.2 Asymmetrische Verschlüsselung

Bei einer asymmetrischen Verschlüsselung werden zum Ver- und Entschlüsseln verschiedene Schlüssel benutzt. Jeder potentielle Empfänger erzeugt ein Schlüsselpaar, welches aus einem öffentlichen und einem privaten Schlüssel besteht. Der Sender verwendet zum Verschlüsseln einer Nachricht den öffentlichen Schlüssel, der vom Empfänger veröffentlicht und allen zur Verfügung gestellt wird. Der Empfänger ist der einzige, der den Geheimtext mit seinem privaten Schlüssel, den er geheim hält, entschlüsseln kann. Da der Chiffrierschlüssel öffentlich zugänglich ist, ist kein vorheriger Schlüsselaustausch nötig. Asymmetrische Verfahren werden auch als Public-Key-Verfahren bezeichnet.

Das erste asymmetrische Verfahren wurde 1976 von Whitfield Diffie und Martin Hellman, in ihrer Arbeit *New Directions in Cryptography*, vorgeschlagen, doch sie konnten keine konkrete Realisierung angeben. In dieser Arbeit lösten sie aber ein anderes Problem. Sie stellten ein Verfahren vor, das einen sicheren Schlüsselaustausch ermöglichte.[37]

[37] Vgl. Beutelspacher (2002), S. 52ff.

2.2.1 Diffie-Hellman-Schlüsselaustausch

Mit dem Verfahren von Diffie und Hellman können zwei Personen einen geheimen Schlüssel über eine unsichere, das heißt öffentliche, Verbindung vereinbaren.

Zuerst wählen die zwei Personen, A und B, eine Primzahl p und eine natürliche Zahl $g < p$. Diese Zahlen können öffentlich bekannt sein. Danach wählen A und B jeweils eine natürliche Zahl a bzw. b mit $a, b < p-1$, die sie geheim halten. A berechnet nun die Zahl

$$\alpha = g^a \bmod p$$

und schickt diese öffentlich an B. B berechnet

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

und schickt diese Zahl auch öffentlich an A. Schließlich berechnet A die Zahl

$$k_A = \beta^a \bmod p$$

und B berechnet

$$k_B = \alpha^b \bmod p.$$

Da

$$k_A = \beta^a \bmod p = (g^b \bmod p)^a \bmod p = (g^b)^a \bmod p = (g^a)^b \bmod p = \\ = (g^a \bmod p)^b \bmod p = \alpha^b \bmod p = k_B$$

ist, erhalten beide die gleiche Zahl, die sie als geheimen Schlüssel verwenden können.

Ein Angreifer kann die Zahlen p, g, α und β abhören, da diese über eine öffentliche Verbindung ausgetauscht werden. Um den geheimen Schlüssel k zu erhalten, müsste er $k = g^{ab} \bmod p$ berechnen. Er kann versuchen, aus den Zahl α bzw. β auf die geheimen Zahlen a bzw. b zu schließen, indem er die beiden Gleichungen

$$\alpha = g^a \bmod p \Leftrightarrow g^a = \alpha \bmod p \Leftrightarrow a = log_g(\alpha) \bmod p$$
$$\beta = g^b \bmod p \Leftrightarrow g^b = \beta \bmod p \Leftrightarrow b = log_g(\beta) \bmod p$$

nach a bzw. b auflöst. Mit diesen beiden Zahlen wäre es dann sehr leicht, den gehei-

men Schlüssel zu bestimmen. Würde man die Gleichungen in den reellen Zahlen auflösen, wäre es mit dem Logarithmus kein Problem. Aber in der modularen Arithmetik ist die Berechnung der sogenannten *diskreten Logarithmusfunktion* mit erheblichem Rechenaufwand verbunden und nach heutigem Wissensstand, für große Zahlen, praktisch nicht durchführbar. Man spricht in diesem Zusammenhang auch häufig vom *Problem des diskreten Logarithmus*.

Nehmen wir an, dass sich A und B zum Beispiel auf die öffentlichen Zahlen $p = 7$ und $g = 2$ geeinigt haben. A wählt als geheime Zahl $a = 2$ und B wählt $b = 4$. A berechnet

$$\alpha = g^a \bmod p = 2^2 \bmod 7 = 4$$

und sendet $\alpha = 4$ an B. B berechnet

$$\beta = g^b \bmod p = 2^4 \bmod 7 = 2$$

und schickt $\beta = 2$ an A. Sie erhalten den geheimen Schlüssel

$$k = g^{ab} \bmod p = 2^{2 \cdot 4} \bmod 7 = 2^8 \bmod 7 = (2^4)^2 \bmod 7 = 2^2 \bmod 7 = 4.$$

Ein Angreifer weiß nun, dass

$$2^a \bmod 7 = 4 \text{ und } 2^b \bmod 7 = 2$$

ist. Die Berechnung der Potenzen ist einfach, aber bis heute kennt man keinen effizienten Algorithmus, um den diskreten Logarithmus zu bestimmen. Der Angreifer kann a und b nur ermitteln, indem er alle in Frage kommenden Exponenten ausprobiert, bis er die gewünschten Ergebnisse $\alpha = 4$ und $\beta = 2$ erhält:

$$\begin{array}{llll} x = 0\text{:} & 2^0 \bmod 7 = 1 & x = 3\text{:} & 2^3 \bmod 7 = 1 \\ \boldsymbol{x = 1}\text{:} & 2^1 \bmod 7 = \mathbf{2} & x = 4\text{:} & 2^4 \bmod 7 = 2 \\ \boldsymbol{x = 2}\text{:} & 2^2 \bmod 7 = \mathbf{4} & x = 5\text{:} & 2^5 \bmod 7 = 4, \end{array}$$

wobei das x sowohl a als auch b repräsentiert. In unserem Beispiel muss er gar nicht alle sechs Möglichkeiten für a, $b < p - 1 = 6$ ausprobieren, da die von $g = 2$ erzeugte

Untergruppe $\langle g \rangle$ von $\mathbb{Z}_7$ nur aus 3 Elementen $\langle 2 \rangle = \{1, 2, 4\}$ besteht. Das heißt, dass der Angreifer nur drei Exponenten durchprobieren muss, um die geheimen Zahlen a und b zu bestimmen. Damit kann er sich dann den geheimen Schlüssel

$$k = g^{ab} \bmod p = 2^{2 \cdot 1} \bmod 7 = 4$$

berechnen. Obwohl der Angreifer für b nicht, wie ursprünglich von B ausgewählt, die Zahl 4 sondern 1 einsetzt, erhält er den gleichen Schlüssel wie A und B, weil $2^{2 \cdot 4} \equiv 2^{2 \cdot 1} \bmod 7$ ist.[38]

Wir haben gesehen, dass ein Angreifer, der die diskreten Logarithmen in $\mathbb{Z}_p \setminus \{0\}$ bestimmen kann, auch den geheimen Schlüssel k von A und B berechnen kann. Um die Sicherheit zu erhöhen, sollte die Zahl g so gewählt werden, dass sie eine möglichst große Untergruppe von $\mathbb{Z}_p \setminus \{0\}$ erzeugt. Wählt man g als erzeugendes Element der zyklischen Gruppe $(\mathbb{Z}_p \setminus \{0\}, \cdot)$, dann gilt $\langle g \rangle = \mathbb{Z}_p \setminus \{0\}$. Somit kommen alle Zahlen zwischen 1 und $p - 1$ als Ergebnis der modularen Potenz $g^a \bmod p$ in Frage. Zudem sollte die Primzahl p so groß gewählt werden, dass die Berechnung des diskreten Logarithmus „praktisch unmöglich" ist. In der Praxis wählt man Primzahlen, die binär dargestellt eine Länge zwischen 1024 und 2048 Bit[39] haben. Ein Angreifer müsste bis zu 2^{1023} bzw. 2^{2047} Zahlen ausprobieren, um den richtigen Exponenten zu finden.[40]

Die Sicherheit des Diffie-Hellman-Schlüsselaustauschs beruht darauf, dass das modulare Potenzieren, die *diskrete Exponentialfunktion*, eine *Einwegfunktion* ist. Eine Einwegfunktion ist eine Funktion, die sich leicht berechnen lässt, ihre Umkehrung aber im allgemeinen große Schwierigkeiten bereitet. Man weiß aber bis heute nicht, ob es andere Möglichkeiten zur Bestimmung des geheimen Schlüssels gibt, ohne diskrete Logarithmen zu berechnen. Solange keine andere Möglichkeit eines Angriffs gefunden wird, ist der Diffie-Hellman-Schlüsselaustausch ein sicheres Verfahren.

[38] Vgl. Freiermuth et al. (2010), S. 201f.
[39] Das sind Zahlen, die über 300 Dezimalstellen haben.
[40] Vgl. Freiermuth et al. (2010), S. 202, Schwenk (2014), S. 18 und Ertel (2012) S. 197

2.2.2 RSA-Verfahren

Das bekannteste asymmetrische Verfahren ist das von Ronald Rivest, Adi Shamir und Len Adleman 1977 entwickelte RSA-Verfahren, das nach den Initialen seiner Erfinder benannt ist.

Wie bereits erwähnt, benötigt man bei der asymmetrischen Verschlüsselung einen Chiffrier- und einen Dechiffrierschlüssel. Bevor eine Nachricht ver- oder entschlüsselt werden kann, muss zuerst jeder Teilnehmer ein entsprechendes Schlüsselpaar erzeugen. Die Schlüsselerzeugung kann entweder von jedem Teilnehmer selbst vorgenommen werden oder von einer Schlüsselerzeugungszentrale erfolgen.

Bei der Schlüsselerzeugung wählt jeder Teilnehmer zwei große Primzahlen p und q und bildet die Produkte

$$n = pq \text{ und } m = (p-1)(q-1).$$

Dann wählt er eine natürliche Zahl e, die teilerfremd zu m ist, das heißt mit

$$ggT(e, m) = 1 \quad .$$

Schließlich berechnet er eine natürliche Zahl d mit

$$ed \bmod m = 1.$$

Weil $ggT(e, m) = 1$ ist, ist e in $\mathbb{Z}_m$ invertierbar und d das zu e inverse Element. Dieses erhält man, indem man mit dem erweiterten Euklidischen Algorithmus Zahlen d und v mit $d \cdot e + v \cdot m = 1$ berechnet[41]. Das Zahlenpaar (e, n) ist der öffentliche Schlüssel des Teilnehmers und d sein privater Schlüssel.

Zum Verschlüsseln einer Nachricht muss diese zuerst als eine oder mehrere natürliche Zahlen $a < n$ dargestellt werden, da das RSA-Verfahren Zahlen in Zahlen verschlüsselt. Der Sender benutzt nun den öffentlichen Schlüssel (e, n) vom Empfänger und berechnet

[41] Vgl. Satz 13

$$c := a^e \bmod n.$$

Er sendet den Geheimtext c an den Empfänger. Der Empfänger berechnet mit seinem privaten Schlüssel d

$$a = c^d \bmod n$$

und erhält den Klartext.

Um nachzuweisen, dass der Empfänger korrekt entschlüsselt, werden wir noch zeigen, dass die Zahl, die der Empfänger berechnet hat, die gleiche Zahl ist, die ursprünglich vom Sender verschickt wurde. Da

$$a = c^d \bmod n = (a^e)^d \bmod n = a^{ed} \bmod n$$

ist, müssen wir zeigen, dass $a \equiv a^{ed} \bmod n$ für alle natürlichen Zahlen $a < n$ gilt. Da wir d mit $d \cdot e + v \cdot m = 1$ berechnet haben ist

$$a^{ed} = a^{1-v \cdot m} = a \cdot a^{-vm} = a \cdot (a^m)^{-v} = a \cdot (a^{(p-1)(q-1)})^{-v}.$$

Wenn $a = 0$ ist, dann ist $a^{ed} = 0$. Für $a \neq 0$ gelten nach Satz 16 (Kleiner Satz von Fermat) folgende Kongruenzen:

$$\begin{aligned} a^{ed} &\equiv a \cdot (a^{(p-1)(q-1)})^{-v} \equiv a \cdot (a^{p-1})^{-v(q-1)} \equiv a \cdot 1^{-v(q-1)} \equiv a \bmod p \\ a^{ed} &\equiv a \cdot (a^{(p-1)(q-1)})^{-v} \equiv a \cdot (a^{q-1})^{-v(p-1)} \equiv a \cdot 1^{-v(p-1)} \equiv a \bmod q \end{aligned}$$

Das bedeutet, dass $a^{ed} - a$ sowohl von p als auch von q geteilt wird. Da p und q verschiedene Primzahlen sind, gilt somit auch, dass $a^{ed} - a$ von $pq = n$ geteilt wird. Das heißt $a^{ed} \equiv a \bmod n$.[42]

An einem einfachen Zahlenbeispiel soll das RSA-Verfahren veranschaulicht werden:

Ein Teilnehmer A wählt zwei verschiedene Primzahlen $p = 13$ und $q = 7$. Dann ist

[42] Vgl. Karpfinger und Kiechle (2010), S. 113

$$n = 13 \cdot 7 = 91 \text{ und } m = 12 \cdot 6 = 72.$$

Dann wählt er eine Zahl e, die teilerfremd zu $m = 72$ ist, zum Beispiel $e = 5$. Er kann nun das multiplikative Inverse von e modulo m berechnen, indem er mit dem erweiterten Euklidischen Algorithmus d und $v \in \mathbb{Z}$ mit $d \cdot e + v \cdot m = 1$ wie folgt bestimmt:

$e = 5$	$m = 72$	
0	1	72
1	0	5
-14	1	2
29	-2	1

Damit ist $29 \cdot 5 + (-2) \cdot 72 = 1$ und $d = 29$ das zu e inverse Element. A veröffentlicht seinen öffentlichen Schlüssel $(e, n) = (5, 91)$, $d = 29$ ist sein geheimer Schlüssel.

Ein Teilnehmer B möchte A zum Beispiel die Nachricht „RSA" senden. Dazu muss er zuerst die Buchstaben durch Zahlen ersetzten. Wie bereits in anderen Beispielen zuvor, ordnen wir dem Alphabet die Zahlen 0 bis $n - 1$ zu und erhalten die Zahlenfolge 17 18 0. Danach verschlüsselt er mit dem öffentlichen Schlüssel von A die Nachricht. Da die Nachricht $a < n$ sein muss, verschlüsselt er die Buchstaben einzeln wie folgt:

$$\begin{aligned} 17^5 &\equiv 75 \bmod 91 \\ 18^5 &\equiv 44 \bmod 91 \\ 0^5 &\equiv 0 \bmod 91 \end{aligned}$$

Nun kann er den Geheimtext „75 44 0" an A senden. A wendet darauf seinen privaten Schlüssel $d = 29$ an

$$\begin{aligned} 75^{29} &\equiv 17 \bmod 91 \\ 44^{29} &\equiv 18 \bmod 91 \\ 0^{29} &\equiv 0 \bmod 91 \end{aligned}$$

und erhält so den Klartext zurück.

Ein Angreifer könnte versuchen, aus dem öffentlichen Schlüssel (n, e), den geheimen Schlüssel d zu berechnen. Damit könnte er, genauso wie der Empfänger, die Nachricht c entschlüsseln. Falls es ihm gelingt, die Zahl $m = (p-1)(q-1)$ zu ermitteln, kann er mit

dem erweiterten Euklidischen Algorithmus den geheimen Schlüssel leicht bestimmen. Dazu müsste er n in seine zwei Primfaktoren p und q zerlegen. Doch bis heute gibt es, wie auch bei der diskreten Logarithmusfunktion, keinen effizienten Algorithmus für die Faktorisierung von großen Zahlen. Die einzige Möglichkeit besteht darin, für jede Primzahl, die kleiner als $\sqrt{n}$ ist zu testen, ob diese ein Teiler von n ist. Wenn n groß genug ist, liegt auch hier eine Einwegfunktion vor. Es ist zwar einfach, zwei große Zahlen zu multiplizieren, aber praktisch unmöglich, eine große Zahl wieder in ihre Primfaktoren zu zerlegen[43]. Für ein sicheres RSA-Verfahren wird empfohlen, p und q so groß zu wählen, dass n, binär dargestellt, eine Länge von mindestens 1024 Bit hat. Bis heute weiß man aber nicht, ob es auch andere Methoden, außer das Faktorisieren von n gibt, um das RSA-Verfahren zu brechen. Das bedeutet, dass das RSA-Verfahren so lange sicher ist, bis ein effizienter Algorithmus für die Faktorisierung von großen Zahlen gefunden wird oder eine andere, noch unbekannte Methode zum Knacken des Verfahres entdeckt wird.

Wie bereits erwähnt, ist im Gegensatz zu symmetrischen Verfahren, bei asymmetrischen Verfahren kein Schlüsselaustausch vor der Kommunikation nötig. Damit ist auch eine spontane Kommunikation zwischen zwei Gesprächspartnern möglich, auch wenn sie sich zuvor nie begegnet sind. Ein weiterer Vorteil ist das einfachere Schlüsselmanagement. Bei symmetrischen Verschlüsselungen benötigen n Teilnehmer $\binom{n}{2} = n(n-1)/2$ Schlüssel. Wobei bei asymmetrischen Verfahren jeder Teilnehmer nur zwei Schlüssel benötigt, somit braucht man $2n$ Schlüssel oder n Schlüsselpaare. Desweiteren können neue Teilnehmer problemlos hinzugefügt werden. Bei symmetrischen Verfahren hingegen müssen alle anderen Teilnehmer einen Schlüssel mit ihm austauschen. Im Vergleich zu symmetrischen Verfahren, die sich sehr effizient implementieren lassen, sind asymmetrische Verfahren jedoch um ein Vielfaches langsamer. Deshalb ist die Verschlüsselung von großen Datenmengen mit asymmetrischen Verfahren viel zu aufwändig. In der Praxis verwendet man daher *Hybridverfahren*, die die Vorteile der symmetrischen und asymmetrischen Verschlüsselung kombinieren.[44] Bei diesen Verfahren wird die Nachricht mit einem symmetrischen Verfahren verschlüsselt. Der Schlüssel, der dabei verwendet wird, wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt, also mit einem asymmetrischen Verfahren. Beides wird an den Empfänger übertragen. Der Empfänger kann den Schlüssel mit seinem geheimen Schlüssel entschlüsseln und diesen dann benutzen, um den Klartext zu erhalten.

[43] Vgl. Schwenk (2014), S. 19
[44] Vgl. Karpfinger und Kiechle (2010), S. 115

3 Kryptologie im Schulunterricht

3.1 Lehrplanbezug

Ein Einblick in die österreichischen Lehrpläne zeigt, dass Kryptologie in verschiedenen Schultypen und Schulstufen thematisiert werden kann. In diesem Abschnitt verweisen sämtliche kursiv geschriebene Textpassagen auf die Lehrpläne RIS (2018), RIS (2019) bzw. RIS (2011).

NMS und AHS-Unterstufe

Bereits in den Lehrplänen der NMS[1] und AHS-Unterstufe[2] wird im Unterrichtsfach Digitale Grundbildung im Lehrstoff das *Verwenden, Erstellen und Reflektieren von Codierungen* als verbindlicher Inhalt genannt. Als Beispiel wird auch die *Geheimschrift* angegeben. Die didaktischen Grundsätze im Mathematikunterricht sehen unter anderem vor, dass die Schüler die *Nützlichkeit der Mathematik in verschiedenen Lebens- und Wissensbereichen* erfahren sollen. Es soll eine *Querverbindung zu anderen Unterrichtsgegenständen sowie Lebenswelt* der Schüler hergestellt werden.

In der Kryptologie ist ein klarer Alltagsbezug gegeben, anhand welchem die Schüler die Nützlichkeit der Mathematik erfahren. Es dürfte jedem Schüler klar sein, weshalb manche Nachrichten (Militär, Bank, usw.) geheim bleiben sollten. Da sie selbst einige Verfahren entdecken können, ist die Motivation für dieses Thema für einige Schüler bestimmt hoch.

[1] Vgl. RIS (2018)
[2] Vgl. RIS (2019)

Blickt man auf fächerübergreifende Aspekte, so ist insbesondere ein enger Bezug zur Informatik vorhanden. Auch geschichtlich ist die Relevanz der Kryptologie sehr hoch und das Thema kann gut mit historischen Aspekten verknüpft werden. Mit der Häufigkeitsanalyse ist sogar eine Verknüpfung der Mathematik mit Sprachen (vor allem Deutsch oder Englisch) möglich.

In der NMS bzw. der AHS-Unterstufe sind alle symmetrischen Verschlüsselungsverfahren denkbar. Die Skytale ist durch den spielerischen Zugang besonders gut für die jüngeren Schüler geeignet, durch das eigenständige Probieren kann Freude an der Thematik geweckt werden. Die der Skytale zugrunde liegende Mathematik beschäftigt sich hauptsächlich mit Permutationen, was Schülern in diesem Alter keine groben Schwierigkeiten bereiten sollte.

Für die Caesar-Verschlüsselung ist die Division mit Rest (bekannt aus der Grundschule) und relative Häufigkeiten bzw. Prozentrechnung (2. Klasse) notwendig. Also sind auch hier die erforderlichen mathematischen Kenntnisse nicht allzu hoch.

Die polyalphabetische Verschlüsselung mit dem Beispiel der Vigenère-Verschlüsselung ist am Ende der AHS-Unterstufe bzw. NMS möglich. Benötigt wird hier der größte gemeinsame Teiler, den die Schüler aus der 2. Klasse kennen. Der Umfang der Kryptoanalyse der Vigenère-Verschlüsselung ist jedoch etwas größer, weshalb die Behandlung der Kryptoanalyse eher in der Oberstufe sinnvoll ist.

AHS-Oberstufe

Im Lehrplan der AHS-Oberstufe[3] ist das mathematische Teilgebiet Kryptologie nicht explizit vorhanden. Die Bildungs- und Lehraufgabe im Mathematikunterricht sieht aber unter anderem vor, dass der Unterricht aufzeigen soll, *dass Mathematik in vielen Bereichen des Lebens (Finanzwirtschaft, Soziologie, Medizin, ...) eine wichtige Rolle spielt.*

In den didaktischen Grundsätzen wird außerdem erwähnt, dass *anwendungsorientierte Kontexte die Nützlichkeit der Mathematik in verschiedenen Lebensbereichen verdeutlichen und so dazu motivieren, neues Wissen und neue Fähigkeiten zu erwerben.*

[3] Vgl. RIS (2019)

In der Tat ist die Kryptologie ein Thema, das im Alltag sehr wichtig ist. Betrachtet man ganz alltägliche Abläufe wie das Verschicken einer Nachricht über das Handy oder das Abheben von Geld bei einem Automaten, so kommt man nicht um Verschlüsselungen herum. Wird den Schülern dies bewusst gemacht, so ist bestimmt ein nötiges Grundinteresse gegeben, zu erfahren, wie Verschlüsselungen funktionieren. Außerdem haben bestimmt schon einige Schüler einem Freund eine Nachricht übermittelt, die „streng geheim" bleiben sollte. Mit den zu besprechenden Verschlüsselungsverfahren ist die Geheimhaltung einer Nachricht nun tatsächlich möglich.

Wie in den didaktischen Grundsätzen formuliert wird, ist die Nützlichkeit der Mathematik etwas, was den Schüler unbedingt nahegelegt werden muss. Der alltägliche Gebrauch sowie die ständige Optimierung von Verschlüsselungsverfahren untermauert diesen Standpunkt sehr gut, und auch die Schüler werden wohl kaum am Nutzen dieses Mathematik-Gebiets zweifeln.

Wird ein Text explizit verschlüsselt, so werden einige Teilgebiete des Lehrplans gebraucht, wie etwa Potenzen, der größter gemeinsamer Teiler oder die Division mit Rest. Auch eine Verbindung mit der Kombinatorik und Stochastik lässt sich erstellen, weil die Sicherheit eines Verschlüsselungsverfahrens zum Beispiel von der Anzahl der Schlüssel abhängt.

Für das Wahlpflichtfach Mathematik beinhaltet der Lehrplan die Fachgebiete *Teilbarkeit, Kongruenz und Kryptologie* als Möglichkeiten zur Vertiefung und Erweiterung des Regelunterrichts. Dementsprechend ist dieses Thema insbesondere bei einem Wahlpflichtfach gut als Unterrichtssequenz realisierbar.

Neben den symmetrischen Verschlüsselungsverfahren, die bereits in der NMS bzw. AHS-Unterstufe behandelt werden können, sind in der AHS-Oberstufe auch asymmetrische Verschlüsselungsverfahren eine Möglichkeit für den Unterricht. Da jedoch der Logarithmus und die detaillierte Behandlung der Potenzen erst in der 6. Klasse erfolgt, sollten diese Verfahren eher erst ab der 7. Klasse im Lehrstoff vorkommen. Dies gilt insbesondere dann, wenn die Sicherheit des Diffie-Hellman-Verfahrens ein Thema sein soll, weil der diskrete Logarithmus und seine schwere Bestimmbarkeit die Basis für die Sicherheit liefert.

Möchte man das RSA-Verfahren mit dem erweiterten Euklidischen Algorithmus anwenden, so bietet sich die Umsetzung der Unterrichtssequenz, wie bereits erwähnt, eher im Wahlpflichtfach Mathematik an, weil die mathematischen Grundlagen den zeitlichen Rahmen des regulären Unterrichts bestimmt sprengen würden.

Höhere Lehranstalt für Informatik bzw. Informationstechnologie

In speziellen Zweigen von höheren technischen Lehranstalten wie die Höhere Lehranstalt für Informatik bzw. Informationstechnologie werden im Lehrplan[4] unter anderem folgende Bereiche im vierten Jahrgang des Pflichtfachs angewandte Mathematik erwähnt:

- *Restklassen*
- *Algebraische und zahlentheoretische Grundlagen der Codierung und Chiffrierung, symmetrische und asymmetrische Verschlüsselung.*
- *Permutationen*

Hier können wir erkennen, dass in bestimmten Schulformen die Kryptologie bereits im Pflichtbereich als fester Bestandteil im Lehrplan verankert ist.

3.2 Unterrichtssequenz

In diesem Abschnitt sollen ausgewählte Verfahren und eine mögliche Umsetzung im Unterricht (im Wahlfach Mathematik für die AHS-Oberstufe) vorgestellt werden. Die Reihenfolge der Verfahren orientiert sich an der Geschichte der Kryptologie. Die Verschlüsselungsverfahren werden zuerst erarbeitet bzw. vorgestellt und nacheinander gebrochen. Die Schwachstelle, die das jeweilige Verfahren aufzeigt, wird mit dem nächsten Verschlüsselungsverfahren beseitigt. Somit zieht sich ein roter Faden durch die Unterrichtseinheiten.

Die Themen sind nach den Verschlüsselungsverfahren aufgeteilt. Der Zugang ist allgemein gehalten, es wird nur eine Grobstruktur für einen möglichen Unterricht geboten.

[4] Vgl. RIS (2011)

Ein genauer Zeitplan ist nicht vorgegeben, da der zeitliche Rahmen sehr stark von Rahmenbedingungen, wie der Leistungsstärke der Klasse oder der verfügbaren Zeit abhängt. Die Lehrperson soll hier selbst entscheiden, welche Teile dieser Unterrichtssequenz sie auswählen möchte. Der Aufbau besteht aus den Lernzielen, eventuell benötigten Materialien, der Vorgehensweise und Bemerkungen. Des Weiteren kann die Sequenz auch auf mehrere Jahre aufgeteilt werden oder an einem Stück abgehalten werden.

Mathematische Beispiele werden in diesem Teil nicht mehr explizit besprochen. Im Anhang sind Arbeitsblätter mit Aufgaben zur Kryptologie zu finden. Die zugrunde liegende Theorie wird als bekannt vorausgesetzt bzw. wird auf die Kapitel 1 und 2 dieser Arbeit verwiesen.

3.2.1 Skytale

Lernziele:

- Die Schüler können Nachrichten mit der Skytale ver- und entschlüsseln.

Materialien:

- Holz-, Papier- oder Schaumstäbe mit verschiedenen Umfängen
- Papierstreifen mit Geheimtext, die mit diesen Stäben erzeugt wurden.
- Leere Papierstreifen
- Arbeitsblatt 1: Skytale

Vorgehensweise:

Die Schüler erhalten Stäbe mit verschiedenen Umfängen und Papierstreifen mit Geheimtexten. Sie sollen in Gruppen herausfinden, welche Botschaften hinter den Papierstreifen verborgen sind.

Danach sollen die Schüler selbst Nachrichten mit einem Stab verschlüsseln und sie an einen anderen Schüler weitergeben, damit dieser die Nachricht entschlüsselt. Die Schüler sollen hier erkennen, wie verschlüsselt und entschlüsselt wird und welche Information der Empfänger benötigt, um die Nachricht richtig zu entschlüsseln.

Nun sollen die Schüler sich Gedanken darüber machen, wie man eine Nachricht auf dieselbe Weise verschlüsseln kann, auch wenn kein Holzstab zur Verfügung steht. Die Schüler verschlüsseln nun eigene Nachrichten, indem sie diese zeilenweise anschreiben und spaltenweise auslesen. Ein Mitschüler soll versuchen diese Nachricht zu entschlüsseln. Auch hier sollen die Schüler erkennen, dass der Empfänger die Anzahl der Zeilen benötigt, um die Nachricht zu entschlüsseln.

Die Lehrperson kann an dieser Stelle die Permutation einführen.

Abschließend recherchieren die Schüler im Internet historische Details zu diesem Verfahren.

Hintergründe/Bemerkungen:
Als Einführung in das Thema Kryptologie bietet sich die Skytale sehr gut an. Einerseits ist die Skytale die älteste und bekannteste Methode, die bereits im 5. Jahrhundert v. Chr. angewendet wurde, was für viele Schüler sehr interessant sein könnte. Andererseits ist diese Methode zur Verschlüsselung von Texten denkbar einfach und sollte für die meisten Schüler schnell begreiflich sein. Zudem wird durch den spielerischen Einstieg das Interesse der Schüler geweckt. Die Motivation der Schüler wird zusätzlich durch das endeckende Lernen gefördert.

Mit geeigneten Fragen führt die Lehrperson die Schüler auf das richtige Ergebnis.

Die Schüler sollen anhand des historischen Aspektes sehen, dass die Skytale praktische Anwendung fand.

Wird der Unterricht computerunterstützt durchgeführt, können die Schüler ihre Nachrichten mit den folgenden Online-Tools ver- und entschlüsseln oder ihre Ergebnisse überprüfen:

Online-Tools *(Stand 1. August 2019):*

- `https://www.cryptool.org/de/cto-chiffren/skytale`[5]

[5] Der Schlüssel ist hier die Anzahl der Spalten.

- `http://kryptografie.de/kryptografie/chiffre/skytale.htm`[6]
- `https://gc.de/gc/skytale/`[7]

3.2.2 Caesar-Verschiebung

Lernziele:

- Die Schüler kennen den Unterschied zwischen Transposition und Substitution.
- Die Schüler können mit der Caesar-Verschiebung Nachrichten ver- und entschlüsseln.
- Die Schüler können mit der Brute-Force-Attacke und der Häufigkeitsanalyse die Caesar-Verschiebung knacken.
- Die Schüler erkennen die Schwäche des Caesar-Verfahrens.
- Die Schüler können die Definition von Restklasse und Kongruenz erklären und können mit Restklassen rechnen.

Materialien:

- Selbstgebastelte Chiffrierscheibe (Vorlage im Anhang)
- Vigenère-Quadrat (siehe Seite 40)
- Häufigkeitsverteilung der Buchstaben der deutschen Sprache (siehe Seite 33)
- Arbeitsblatt 2: Häufigkeitsanalyse

Vorgehensweise:

Die Lehrperson schreibt einen mit Caesar verschlüsselten Text auf die Tafel:

`GLHVH QDFKULFKW LVW JHKHLP`

Die Schüler sollen versuchen, den Text zu brechen. Die Schüler, die es schaffen den Text zu knacken dürfen nacheinander jeweils einen Buchstaben des Klartextes nennen,

[6] Hier muss darauf geachtet werden, dass die Leerzeichen bei der Eingabe entfernt werden. Ausgegeben werden alle möglichen Klar- bzw. Geheimtexte mit der Anzahl der Spalten.
[7] Der Umfang entspricht hier der Anzahl der Spalten.

bis die gesamte Nachricht entschlüsselt ist. Die entschlüsselte Nachricht lautet: „Diese Nachricht ist geheim". Der Schlüssel ist $C = 3$.

Die Schüler sollen erkennen, dass mit einem verschobenen Alphabet verschlüsselt wurde. Danach sollen sie eigene Texte (mithilfe einer zuvor selbst gebastelten Chiffrierscheibe oder dem Vigenère-Quadrat) verschlüsseln und diese an einen Mitschüler weitergeben, damit dieser den Text entschlüsselt. Die Schüler sollen hier erkennen, dass der Empfänger wissen muss, um wie viele Stellen das Klartextalphabet verschoben wurde, damit sie die Nachricht entschlüsseln können.

An dieser Stelle führt die Lehrperson die Begriffe Kyptologie, Kryptoanalyse, Kryptrographie, Klartext, Geheimtext, Schlüssel, Verschlüsseln (Chiffrieren), Entschlüsseln (Dechiffrieren), Angriff und Brechen bzw. Knacken einer verschlüsselten Nachricht ein.

Die Schüler sollen nun in eigenen Worten erklären, inwiefern sich die Verschlüsselung mit der Skytale von der Caesar-Verschiebung unterscheidet.

Als Nächstes führt die Lehrperson die Begriffe Transposition und Substitution ein.

An dieser Stelle wird das Verfahren mathematisch erfasst. Dazu führt die Lehrperson zuerst Modulares Rechnen, Kongruenz und Restklasse ein. Den Schülern werden ein paar Aufgaben zum Üben gegeben, bevor die Caesar-Verschiebung durch eine Funktion beschrieben wird.

Die Schüler können dann die Nachricht, die sie zuvor verschlüsselt haben, mit der modularen Addition verschlüsseln und die des Partners mit der modularen Subtraktion entschlüsseln.

Die Schüler sollen sich nun Gedanken darüber machen, wie man eine Nachricht, die mit Caesar verschlüsselt wurde, entschlüsseln kann, wenn man nicht weiß, um wie viele Stellen das Alphabet verschoben wurde. Sie werden schnell erkennen, dass es 25 mögliche Schlüssel gibt, die man nacheinander ausprobieren kann. Sie sehen, dass die Verschlüsselung dadurch leicht gebrochen werden kann.

Um nun noch auf die Häufigkeitsanalyse einzugehen, stellt die Lehrperson die Frage, ob

es eine andere Möglichkeit als das Durchprobieren aller Schlüssel gibt. Bevor die Schüler diese Frage beantworten, sollen sie die Häufigkeit der Buchstaben von den Nachrichten zählen, die sie gegenseitig ausgetauscht haben. Diese werden auf der Tafel notiert. Zu erwarten ist, dass die Buchstaben e und n am Häufigsten auftreten. Den Schülern wird erklärt, dass in der deutschen Sprache diese Buchstaben am häufigsten vorkommen.

Die Schüler sollten nun in er Lage sein, die zuvor gestellte Frage zu beantworten.

Falls die häufigsten Buchstaben nicht wie erwartet e und n sind. Kann sofort auf die Problematik von kurzen Texten eingegangen werden, falls nicht, kann das auch nach der Beantwortung der Frage thematisiert werden.

Die Lehrperson stellt jetzt das Prinzip von Kerckhoffs vor.

Den Schülern kann nun ein längerer Text zum Brechen mit der Häufigkeitsanalyse vorgelegt werden.

Hintergründe/Bemerkungen:
Durch den Rätselcharakter wird auch hier das Interesse der Schüler geweckt. In der Einführungsphase soll der Text Buchstabe für Buchstabe entschlüsselt werden, damit auch die langsameren Schüler die Möglichkeit haben, selbst die Lösung zu entdecken.

Für die Schüler bietet das Basteln einer Chiffrierscheibe eine angenehme Abwechslung zu den sonst eher theoretischen Themen.

Die wichtigsten Begriffe der Kryptologie können hier anhand von einem sehr einfachen Verfahren eingeführt werden.

Bevor das Verfahren mathematisch erfasst werden kann, sollen folgende mathematische Grundlagen geschaffen werden:
Zuerst soll die Definition der Teilbarkeit wiederholt werden. Diese wird benötigt, um Beweise durchführen zu können. Danach wird die Modulo-Operation definiert und durch ein paar Beispiele erläutert. Es folgt die Definition der Kongruenz, welche auch mit Beispielen veranschaulicht und geübt wird. Nun wird die Restklasse definiert. Diese kann zuerst einfach, wie zum Beispiel „alle Zahlen, die den gleichen Buchstaben repräsentie-

ren", und dann allgemein definiert werden. Im Unterricht lässt sich an dieser Stelle auch der Beweis der Gleichheit von Restklassen leicht durchführen. Anschließend sollten die Rechenregeln erläutert und eventuell auch bewiesen werden. Die Rechenregeln für die Addition und die Multiplikation

$$(a+b) \bmod n = (a \bmod n) + (b \bmod n) \text{ und } (a \cdot b) \bmod n = (a \bmod n) \cdot (b \bmod n),$$

sollen auf jeden Fall angesprochen werden. Die zweite Aussage ist vor allem später für den Diffie-Hellman-Schlüsselaustausch von Bedeutung. Den Schülern soll genug Zeit zum Üben gegeben werden. Da bei der Entschlüsselung auch negative Zahlen herauskommen, müssen auch diese zuvor betrachtet werden.

Es bietet sich an, die Häufigkeitsanalyse bereits hier einzuführen, weil die Analyse sehr einfach ist und die Schüler auf dieses Wissen beim Knacken der Vigenère-Verschlüsselung zurückgreifen können.

Falls der längere Geheimtext von den Schülern händisch gebrochen werden soll, ist es sinnvoll, den Text aufzuteilen. Die Schüler können in Gruppen die Buchstaben des Teiltextes zählen und diese dann mit den anderen Gruppen aufsummieren. Um die Arbeit zu reduzieren bietet es sich hier an, in Verbindung mit dem Informatikunterricht ein Programm zu entwickeln, das die Häufigkeiten der Buchstaben zählt. Alternativ existieren auch Online-Tools, die diese Aufgabe erfüllen. Desweitern wird an das Vorwissen der Schüler angeknüpft und es bietet sich hier die Gelegenheit, absolute und relative Häufigkeiten zu wiederholen.

Die Caesar-Verschiebung eignet sich auch sehr gut im Informatikunterricht als Programmierbeispiel.

Online-Tools *(Stand 1. August 2019):*
Ver- und Entschlüsselung mit Caesar:

- `http://kryptografie.de/kryptografie/chiffre/caesar.htm`
- `https://www.cryptool.org/de/cto-chiffren/caesar`
- `https://gc.de/gc/caesar/`

Häufigkeiten der Buchstaben zählen:

- `https://gc.de/gc/buchstabenhaeufigkeit/`

Häufigkeiten der Buchstaben zählen und Häufigkeitsverteilung:

- `http://kryptografie.de/kryptografie/kryptoanalyse/haeufigkeitsverteilung.htm`

3.2.3 Vigenère-Verschlüsselung

Lernziele:

- Die Schüler können mit der Vigenère-Verschlüsselung Nachrichten ver- und entschlüsseln.
- Die Schüler kennen den Unterschied zwischen einer mono- und einer polyalphabetischen Verschlüsselung.
- Die Schüler können erklären, warum mittels einer einfachen Häufigkeitsanalyse ein Geheimtext, welcher mit einem polyalphabetischen Verfahren verschlüsselt wurde, nicht gebrochen werden kann.
- Die Schüler können bei bekannter Schlüsselwortlänge das Schlüsselwort bestimmen.
- Die Schüler können mit dem Kasiski-Test die Schlüsselwortlänge bestimmen.
- Die Schüler können erklären, warum das Verfahren mit einem längeren Schlüsselwort sicherer ist.

Materialien:

- Vigenère-Quadrat (siehe Seite 40)
- Selbstgebastelte Chiffrierscheibe (Vorlage im Anhang)
- Häufigkeitsverteilung der Buchstaben der deutschen Sprache (siehe Seite 33)
- Arbeitsblatt 3: Knacken der Vigenère-Verschlüsselung

Vorgehensweise:

Nachdem die Caesar-Verschiebung gebrochen wurde, wird den Schülern die Vigenère-Verschlüsselung mit einem Beispiel erläutert:

Schlüssel	G	E	H	E	I	M	G	E	H	E	I	M	G	E	H
Klartext	v	i	g	e	n	e	r	e	c	h	i	f	f	r	e
Geheimtext	B	M	N	I	V	Q	X	I	J	L	Q	R	L	V	L

Die Schüler sollen dann ein Schlüsselwort wählen und selbstständig oder in Gruppen einen kurzen, selbst gewählten Text (mithilfe der Chiffrierscheibe oder dem Vigenère-Quadrat) verschlüsseln. Die Geheimtexte werden wieder ausgetauscht und entschlüsselt.

Die Schüler sollen die Vigenère-Verschlüsselung mit einer geeigneten Funktion darstellen und den Text zuvor mit dieser ver- und entschlüsseln.

Die Lehrperson führt jetzt die Begriffe monoalphabetische und polyalphabetische Verschlüsselung ein und erklärt den Unterschied.

Die Schüler sollen sich nun Gedanken darüber machen, ob dieses Verfahren mit der einfachen Häufigkeitsanalyse geknackt werden kann. Sie sollen auch erkennen, dass es zu viele Schlüssel gibt, sodass ein Brute-Force-Angriff nicht sinnvoll ist.

Die Lehrperson kann nun die Häufigkeitsverteilung der Buchstaben eines mit Vigenère verschlüsselten Geheimtextes vorzeigen. Die Schüler sollten hier erkennen, dass die Buchstaben gleichmäßiger verteilt sind. Durch gezielte Andeutungen, wie zum Beispiel (bei einer Schlüsselwortlänge von 5 Buchstaben): „Jeder 5. Buchstabe wurde hier mit einer Caesar-Verschiebung verschlüsselt", kann die Lehrperson die Schüler anleiten, sodass sie erkennen, dass eine Häufigkeitsanalyse auf Teiltexte, die mit demselben Schlüsselwortbuchstaben verschlüsselt wurden, angewendet werden kann.

Die Schüler erhalten nun einen Geheimtext, bei dem sie wissen, wie lang das verwendete Schlüsselwort ist. Der Geheimtext wird in Teiltexte unterteilt. Die Schüler identifizieren den häufigsten Buchstaben pro Teiltext und bestimmen das Schlüsselwort. Mit diesem Schlüsselwort entschlüsseln sie dann den Geheimtext. Wichtig ist, dass die Schüler erkennen, dass die Sprache der Nachricht bekannt sein muss und der Text eine hinreichende Länge haben muss, damit die Häufigkeitsanalyse funktioniert. An dieser Stelle kann auch ein Angriff durch Ausprobieren der möglichen Schlüssellänge angesprochen werden. Man probiert verschiedene Schlüssellängen aus und Anhand der Häufigkeitsver-

teilung der Buchstabengruppen, kann man erkennen, ob man die richtige Länge erraten hat.

Die Lehrperson stellt nun den Kasiski-Test zum Auffinden der Schlüsselwortlänge vor. Danach können die Schüler den Test auf einen Geheimtext anwenden.

Nun sollten Überlegungen mit den Schülern angestellt werden, wie die Bestimmung des Schlüsselwortes erschwert werden kann, um das Verfahren sicherer zu machen.

Hintergründe/Bemerkungen:
Die Einführung der Vigenère-Verschlüsselung kann zum besseren Verständnis auch zuvor mit nur zwei Geheimtextalphabeten erfolgen und erst später mit einem Schlüsselwort erklärt werden.

Beim Ver- und Entschlüsseln mit dem Vigenère-Quadrat ist es sinnvoll, dass die Schüler mit zwei Linealen arbeiten, damit sie nicht in der Zeile bzw. Spalte verrutschen. Wenn sich die Schüler die Geheimtextalphabete mit denen sie arbeiten zuerst rausschreiben, wird ihnen die Ver- und Entschlüsselung wahrscheinlich leichter fallen. Es ist auch hilfreich, wenn die Texte in Teilblöcke aufgeteilt werden, sodass immer nur Teilblöcke, die mit demselben Schlüsselwortbuchstaben ver- oder entschlüsselt werden, bearbeitet werden. In der Gruppe können die Teilblöcke so aufgeteilt werden, dass jedes Gruppenmitglied mit nur einem Geheimtextbuchstaben arbeitet, somit ver- bzw. entschlüsselt jedes Mitglied der Gruppe eigentlich nur mit einem einfachen Caesar-Verfahren. Mit dieser Erkenntnis könnten die Schüler sogar selbstständig darauf kommen, dass die Vigenère-Verschlüsselung mit einer Häufigkeitsanalyse auf die Teilblöcke gebrochen werden kann.

Da die Funktion nur eine Erweiterung der Funktion bei der Caesar-Verschiebung ist, sollten die Schüler diese selbstständig anschreiben können.

Bei einer Brute-Force-Attacke gibt es bei einem Schlüsselwort der Länge zwei $26 \cdot 26$ mögliche Schlüsselkombinationen, bei einer Länge von drei Buchstaben beträgt die Anzahl der möglichen Schlüssel bereits 26^3, usw. Hier können die Schüler schnell erkennen, dass die mögliche Anzahl der Schlüssel sehr schnell sehr groß wird und das Durchprobieren aller möglichen Schlüssel nicht umsetzbar ist.

Wie auch beim Ver- und Entschlüsseln können bei der Bestimmung des Schlüsselwortes bei bekannter Schlüsselwortlänge die Schüler in Gruppen eingeteilt werden, sodass jede Gruppe die Häufigkeitsanalyse für einen Teilblock macht und nur einen Buchstaben des Schlüsselworts bestimmt. Der Geheimtext, den die Schüler hier erhalten, sollte von der Lehrperson so gewählt werden, dass die Häufigkeiten der Buchstaben, dem der deutschen Sprache entsprechen, damit diese dann bei der Häufigkeitsanalyse erfolgsversprechend verwendet werden kann.

Damit die Schüler erkennen, warum die verwendete Sprache für die Häufigkeitsanalyse bekannt sein muss, kann die Lehrperson die Häufigkeitsverteilungen anderer Sprachen noch ansprechen und vorzeigen[8]. Dass die Häufigkeitsanalyse bei sehr kurzen Texten (weniger als 100 Buchstaben) nicht funktioniert, kann die Lehrperson anhand eines sehr kurzen Geheimtextes veranschaulichen.

Die Schüler wissen nun, dass die Vigenère-Verschlüsselung mit bekannter Schlüsselwortlänge geknackt werden kann. Das erhöht die Motivation, ein Verfahren kennenzulernen, mit dem man die Schlüsselwortlänge bestimmen kann.

Beim Durchsuchen von Buchstabenwiederholungen im Geheimtext empfiehlt es sich, ein Online-Tool zu verwenden, da sonst das Suchen sehr viel Zeit in Anspruch nimmt und eventuell dazu führt, dass die Schüler das Interesse verlieren. Die Buchstabenfolgen sollten aus mindestens vier Buchstaben bestehen, damit der Test funktioniert. Nachdem die Schlüsselwortlänge bestimmt ist, kann das Bestimmen des Schlüsselwortes selbst weggelassen werden, da dies bereits in der vorherigen Übung gemacht wurde. Interessierte Schüler können und werden diese Übung zuhause fortsetzen. Die Schüler sehen nun, dass auch die Vigenère-Verschlüsselung gebrochen werden kann.

Je länger das Schlüsselwort ist, desto schwieriger wird das Bestimmen der Schlüsselwortlänge. Im Kasiski-Test kann man beobachten, dass sich bei kurzen Schlüsselwörtern Buchstabenfolgen öfter wiederholen als bei längeren. Die Lehrperson kann die Schüler auf diese Erkenntnis führen, indem sie zum Beispiel fragt, was passiert, wenn das Schlüsselwort gleich lang wie die zu verschlüsselnde Nachricht ist. Die Schüler sollten hier erkennen, dass dann eine Häufigkeitsanalyse der einzelnen Textblöcke nicht machbar ist. Da es schwierig ist lange Wörter zu finden, kommen die Schüler hier wahrscheinlich

[8] zum Beispiel auf der Seite `https://de.wikipedia.org/wiki/Buchstabenhäufigkeit`

selbst auf die Idee, nicht nur einzelne Wörter zu verwenden, sondern einen ganzen Satz bzw. einen Ausschnitt aus einem Buch. Eine mögliche Schülerantwort wäre auch, dass die Geheimtextalphabete nicht nur verschoben werden, sondern beliebige permutierte Alphabete zum Verschlüsseln verwendet werden. Hier besteht die Schwierigkeit darin, dass das Geheimtextalphabet sehr kompliziert wird und dadurch schwer zu merken ist.

Mit folgenden Online-Tools können die Schüler die Aufgaben durchführen bzw. ihre Ergebnisse kontrollieren:

Online-Tools *(Stand 1. August 2019):*
Ver- und Entschlüsseln mit der Vigenère-Verschlüsselung:

- `http://kryptografie.de/kryptografie/chiffre/vigenere.htm`
- `https://gc.de/gc/vigenere/`
- `https://www.cryptool.org/de/cto-chiffren/vigenere`

Häufigkeiten der Buchstaben zählen:

- `https://gc.de/gc/buchstabenhaeufigkeit/`

Häufigkeiten der Buchstaben zählen und Häufigkeitsverteilung:

- `http://kryptografie.de/kryptografie/kryptoanalyse/haeufigkeitsverteilung.htm`

Durchsuchen von Buchstabenwiederholungen im Geheimtext:

- `http://kryptografie.de/kryptografie/kryptoanalyse/kasiski-test.htm`

Knacken der Vigenère-Verschlüsselung:

- `http://www.cryptoprograms.com/subsolve/periodic`

3.2.4 Enigma

Lernziele:

- Die Schüler können die grundlegende Funktionsweise und den Aufbau der Enigma (Grundmodell) erklären.

- Die Schüler können die Anzahl der Permutationen einer gegebenen Menge berechnen.
- Die Schüler können den Binomialkoeffizienten berechnen.
- Die Schüler erkennen, dass der Binomialkoeffizient für die Berechnung von Möglichkeiten verwendet wird.

Materialien:

- Dokumentation: „Wie ein Mathegenie Hitler knackte“
  `https://www.youtube.com/watch?v=l42KX7kYHVY` (Zugriff am 1. August 2019)

Vorgehensweise:

Den Schülern wird ein Filmausschnitt gezeigt. Daraufhin erklärt die Lehrperson wie die Enigma aufgebaut ist und wie sie funktionieret.

Die Lehrperson wiederholt die Permutation und erarbeitet mit den Schülern die Anzahl der Permutationen einer Menge mit n Elementen. Danach erarbeitet sie mit den Schülern den Binomialkoeffizienten an einem Beispiel (z.B. Lotto).

Anschließend wird mit den Schülern die mögliche Schlüsselanzahl des Grundmodells der Enigma berechnet.

Hintergründe/Bemerkungen:

In der Dokumentation geht es hauptsächlich um Alan Turing und im ersten Teil des Films vorwiegend darum, wie er die Enigma knackte und welche Auswirkungen das auf den 2. Weltkrieg hatte. Im Unterricht sollte der Film ungefähr bis zur 28. Minute gezeigt werden. Dadurch sollen die Schüler motiviert werden, mehr über die Funktionsweise der Enigma zu erfahren. Zudem eignet sich der geschichtliche Hintergrund sehr gut als Möglichkeit für einen fächerübergreifenden Unterricht und kann das Interesse geschichtlich interessierter Schüler auf die Mathematik lenken.

Der Aufbau der Enigma sollte, wie in Abschnitt 2.1.2 Enigma, schrittweise erweitert werden, um die Schüler nicht zu überfordern.

Damit die Schüler die Anzahl der Schlüssel berechnen können, muss zuvor die Anzahl

der Permutationen einer bestimmten Menge und der Binomialkoeffizient erarbeitet werden.

Die Schüler sollen erkennen, dass eine sehr große Anzahl an Schlüsseln nicht ausreichend ist, um die Sicherheit eines Verfahrens zu gewährleisten.

3.2.5 One-Time-Pad

Lernziele:

- Die Schüler können das One-Time-Pad mit Buchstaben und Binärzahlen anwenden.
- Die Schüler können erklären, warum das One-Time-Pad ein sicheres Verfahren ist.
- Die Schüler können Dezimalzahlen in Binärzahlen umwandeln und umgekehrt.

Materialien:

- Chiffrierscheibe (Vorlage im Anhang)
- Vigenère-Quadrat (siehe Seite 40)
- ASCII[9]-Tabelle (siehe Anhang)

Vorgehensweise:
Nachdem alle bis jetzt vorgestellten Verfahren geknackt wurden, wird die Frage an die Schüler gestellt, ob es unknackbare Verschlüsselungen gibt. Die Meinungen der Schüler werden eingeholt. Anschließend erklärt die Lehrperson das One-Time-Pad.

Die Lehrperson schreibt einen Geheimtext auf die Tafel:

```
T F Z Z G R E D F Y A B X I F F H X Y
```

Die Schüler sollen diesen in Gruppen entschlüsseln. Dafür bekommt jede Gruppe einen eigenen Schlüssel. Zum Beispiel:

[9] American Standard Code for Information Interchage

```
Schlüssel 1: Q X V H C A M D M Z S J E C B Y D P M
Schlüssel 2: H F G S C F E B Y F F T M X N Q H F G
Schlüssel 3: P X M F T H R D D O Z B G E O M D A F
```

Nach dem Entschlüsseln werden die Ergebnisse verglichen. Nun wird diskutiert, warum das One-Time-Pad unknackbar ist.

An dieser Stelle soll das bitweise Verschlüsseln mit dem One-Time-Pad angesprochen werden. Dazu müssen die Buchstaben zuerst durch Zahlen dargestellt und anschließend in Binärdarstellung umgerechnet werden. Die Lehrperson stellt hier das Dezimal- und das Binärsystem vor und erklärt, wie Zahlen zu jeweils dem anderen System umgerechnet werden. Anschließend stellt die Lehrperson den ASCII-Code vor.

Nun sollen die Schüler eine kurze, selbst gewählte Nachricht verschlüsseln. Zuerst stellen sie die Buchstaben als Binärzahlen dar und verschlüsseln diese mit einer zufällig gewählten Bitfolge. Die Nachrichten werden ausgetauscht und entschlüsselt. Die Lehrperson lässt die Schüler beim Entschlüsseln entdecken, dass die bitweise Subtraktion und die Addition ohne Übertrag das gleiche Ergebnis liefern.

Hintergründe/Bemerkungen:
Wahrscheinlich werden die Schüler an diesem Punkt denken, dass es keine Verschlüsselung gibt, die nicht gebrochen werden kann. Umso überraschender ist es dann, wenn sie ein solches Verfahren kennenlernen.

Zum Entschlüsseln können die Schüler die Chiffrierscheibe oder das Vigenère-Quadrat verwenden. Nach dem Entschlüsseln des Geheimtextes stellen die Schüler fest, dass sie zum gleichen Geheimtext verschiedene Klartexte erhalten haben. Sie sollten nun selbst argumentieren können, warum es keinen Sinn macht, zu versuchen einen Geheimtext, welcher mit dem One-Time-Pad verschlüsselt wurde, zu knacken.

Die Binärdarstellung von Zahlen und der ASCII-Code sollten unbedingt angesprochen werden, da die Verschlüsselungsverfahren heute (am Computer) bitweise betrieben und die Zeichen durch einen 8-Bit-ASCII-Code dargestellt werden. Wenn den Schülern aus der 5. Klasse die verschiedenen Zahlensysteme bereits bekannt sind, bietet sich diese Übung an, um das Gelernte zu wiederholen.

Die Schüler können beim Ver- und Entschlüsseln die Zahlen bzw. Buchstaben entweder selbst in Binärdarstellung umrechnen oder die ASCII-Tabelle benutzen.

Online-Tools *(Stand 1. August 2019):*
Darstellung der Buchstaben in ASCII-Code als Dezimalzahl und umgekehrt:

- `https://gc.de/gc/ascii/`

Umwandlung von positiven ganzen Zahlen in Binärzahlen und umgekehrt:

- `https://gc.de/gc/binaer/`

Umwandlung von Nachrichten in ASCII-Code in Binärdarstellung und umgekehrt:

- `https://www.cryptool.org/de/cto-kodierungen/ascii`

3.2.6 Symmetrische und asymmetrische Verschlüsselung

Lernziele:

- Die Schüler können zwischen symmetrischen und asymmetrischen Verfahren unterscheiden.
- Die Schüler kennen die Schwachstellen der symmetrischen Verschlüsselung und die Vorteile der asymmetrischen Verschlüsselung.
- Die Schüler können die Anzahl der Schlüssel, die zwischen den Teilnehmern ausgetauscht werden müssen, bei symmetrischen und asymmetrischen Verfahren berechnen.

Vorgehensweise:
Die Lehrperson erklärt, dass die bis jetzt kennengelenten Verfahren symmetrisch sind und geht darauf ein, dass bei diesen der Schlüsselaustausch über einen sicheren Kanal eine Voraussetzung ist.

Danach wird auf das Problem der Schlüsselverteilung eingegangen. Mit den Schülern wird nun die Anzahl der Schlüssel, die bei symmetrischen Verfahren zwischen den Kommunikationspartnern ausgetauscht werden müssen, berechnet. Dazu sollen sich die Schüler aufschreiben, wie viele Schlüssel sie benötigen, um mit jedem Mitschüler der Klasse

kommunizieren zu können. Danach wird die Anzahl der Schlüssel für alle Schüler der Klasse berechnet. Aus dieser Erkenntnis wird eine allgemeine Formel hergeleitet.

Die Lehrperson stellt den Schülern das Prinzip der asymmetrischen Verschlüsselung vor. Nun wird auch hier die Anzahl der benötigten Schlüssel berechnet.

Hintergründe/Bemerkungen:
Nachdem die Schüler ein unknackbares Verfahren kennengelernt haben, könnten sie davon ausgehen, dass das Thema Kryptologie damit beendet ist. Nun sollen sie sehen, dass, auch wenn es so ein Verfahren gibt, symmetrische Verschlüsselungen eine sehr große Schwachstelle aufweisen.

Beim One-Time-Pad müsste zuerst ein gleich langer Schlüssel wie der Text ausgetauscht werden, bevor die eigentliche Nachricht verschickt wird. Die Lehrperson soll verdeutlichen, dass auch bei einem einfachen Schlüssel die Teilnehmer zuerst in Kontakt treten müssen, was nicht immer vor einem Nachrichtenaustausch möglich ist, da die Teilnehmer vielleicht viel zu weit voneinander entfernt sind oder sich gar nicht erst kennen.

Die Schüler können das zuvor erlernte Wissen (Binomialkoeffizient) hier noch einmal anwenden und erkennen, dass bereits mit wenigen Teilnehmern, also etwa die Anzahl der Schüler der Klasse, sehr viele Schlüssel ausgetauscht werden müssen. Vergleicht man das mit der Anzahl der Teilnehmer in sozialen Netzwerken, sehen die Schüler einen weiteren Nachteil der symmetrischen Verschlüsselung.

Die Schüler sollen bei den asymmetrischen Verfahren sehen, dass das Problem der Schlüsselverwaltung nicht behoben, aber stark vereinfacht wird.

3.2.7 Diffie-Hellman-Schlüsselaustausch

Lernziele:

- Die Schüler können die Schritte des Diffie-Hellman-Schlüsselaustausches erklären.
- Die Schüler können mit dem Diffie-Hellman-Schlüsselaustausch einen Schlüssel erzeugen.

- Die Schüler können erklären, auf was die Sicherheit des Diffie-Hellman-Schlüsselaustausches beruht.

Vorgehensweise:
Die Schüler bekommen ein paar Beispiele, um das modulare Potenzieren zu üben und lernen durch das Aufteilen des Exponenten große Zahlen zu vermeiden.

Danach werden die Schüler in drei Gruppen aufgeteilt. Die Gruppen A und B sollen einen geheimen Schlüssel austauschen und die Gruppe C soll ihnen dabei zuhören und versuchen, den Schlüssel zu erraten. Die Lehrperson schreibt

$$7^x \bmod 11$$

auf die Tafel. Danach sollen sich die Gruppen A und B jeweils eine Zahl a bzw. b, die beide kleiner als 10 sind, überlegen und geheim halten. Nun berechnet die Gruppe A $7^a \bmod 11 = \alpha$ und die Gruppe B berechnet $7^b \bmod 11 = \beta$. Diese Zahlen tauschen die Gruppen öffentlich aus, indem sie die Zahlen laut aussprechen. Die Lehrperson notiert diese Informationen auf der Tafel. Die Gruppen A und B sollen nun den geheimen Schlüssel berechnen. A berechnet $\beta^a \bmod 11$ und B berechnet $\alpha^b \bmod 11$. Die Gruppen A und B treffen sich nun und vergleichen, ob sie den gleichen Schlüssel haben. Sie müssen aber darauf achten, dass Gruppe C sie nicht hört. Währenddessen ist Gruppe C damit beschäftigt, den geheimen Schlüssel ausfindig zu machen. Nachdem die Gruppe C den Schlüssel auch berechnet hat, soll dieser öffentlich gemacht und verglichen werden.

Gruppe C soll nun erklären, wie sie den Schlüssel berechnet haben.

Die Lehrperson erklärt nun den Diffie-Hellman-Schlüsselaustausch. Es wird gezeigt, warum die Gesprächspartner den gleichen Schlüssel erhalten, obwohl sie verschiedene Berechnungen durchgeführt haben.

Die Lehrperson erklärt den Schülern dann, warum die diskrete Exponentialfunktion nicht so leicht umkehrbar ist, wie es die Exponentialfunktion in den reellen Zahlen ist. Den Schülern wird auch mitgeteilt, dass in der Praxis Zahlen mit über 300 Dezimalstellen gewählt werden und die Umkehrung dadurch praktisch nicht mehr möglich ist.

Hintergründe/Bemerkungen:
Damit später beim Rechnen nicht allzu große Zahlen herauskommen, soll den Schülern im ersten Schritt gezeigt werden, dass durch geschicktes „Klammersetzen" große Zahlen vermieden werden können. Zudem ist es eine gute Gelegenheit, die Rechenregeln für die Potenzrechnung zu wiederholen.

Die Aufteilung der Gruppen sollte so erfolgen, dass die Gruppe C größer ist, da sie wahrscheinlich mehr rechnen müssen als die anderen beiden Gruppen. Die Zahlen sind so gewählt, dass 7 ein Erzeuger der zyklischen Gruppe $\mathbb{Z}_{11} \setminus \{0\}$ ist, damit Gruppe C das Ergebnis nicht zu schnell berechnen kann. Die Lehrperson kann hier der Gruppe C Anleitungen geben, wie sie vorgehen sollen. Jedes Gruppenmitglied sollte eine Zahl ausprobieren und schauen, ob das Ergebnis mit einer der ausgetauschten Zahlen α oder β übereinstimmt und dann den Schlüssel berechnen.

Zu erwarten ist, dass die Gruppe C erklärt, dass sie den Schlüssel durch Ausprobieren gefunden haben. Dadurch erkennen sie später, dass es bei sehr großen Zahlen nicht zielführend ist, durch Probieren den Schlüssel zu finden.

Online-Tools *(Stand 1. August 2019):*
Berechnen des Schlüssels mit Eingabe aller Parameter:

- `https://inf-schule.de/kommunikation/kryptologie/modernechiffriersysteme/exkurs_diffie`

3.2.8 RSA-Verfahren

Lernziele:

- Die Schüler können den Euklidischen und den erweiterten Euklidischen Algorithmus anwenden.
- Die Schüler können die Schlüssel für das RSA-Verfahren erzeugen.
- Die Schüler können Nachrichten mit dem RSA-Verfahren verschlüsseln.
- Die Schüler können einen mit RSA verschlüsselten Geheimtext mit bekanntem geheimen Schlüssel entschlüsseln.

- Die Schüler können erklären, auf was die Sicherheit des RSA-Verfahrens beruht.

Vorgehensweise:
Die Lehrperson erklärt das Prinzip des RSA-Verfahrens anhand eines einfachen Zahlenbeispiels.

Die Schüler lernen den Euklidischen Algorithmus zur Bestimmung des größten gemeinsamen Teilers von zwei Zahlen kennen. Sie berechnen dann anhand von ein paar Beispielen selbstständig den größten gemeinsamen Teiler von zwei Zahlen.

Danach wird das Lemma von Bézout eingeführt und bewiesen, indem zuerst der Euklidische Algorithmus angewendet wird und danach die Gleichungen von unten nach oben aufgelöst werden. Die Lehrperson benennt diese Berechnung als den erweiterten Euklidischen Algorithmus. An einem Beispiel zeigt sie, wie der erweiterte Euklidische Algorithmus effizienter in einer Tabelle angeschrieben werden kann. Die Schüler bekommen dann ein Beispiel zum eigenständigen Rechnen.

Das RSA-Verfahren wird nun schrittweise erarbeitet. Zuerst wird die Schlüsselerzeugung thematisiert und mit kleinen Zahlen durchgerechnet. Dann wird Verschlüsselung und Entschlüsselung einer Nachricht mit dem RSA-Verfahren besprochen und anhand eines Beispiels demonstriert.

Möchte die Lehrperson beweisen, warum nach dem Entschlüsseln wieder die ursprüngliche Nachricht herauskommt, sollte sie an dieser Stelle den kleinen Satz von Fermat einführen und damit die Aussage beweisen.

Die Schüler können nun versuchen, aus einem bekannten öffentlichen Schlüssel den geheimen Schlüssel zu berechnen. Anschließend wird die Sicherheit des RSA-Verfahrens, welches auf der Schwierigkeit der Faktorisierung beruht, besprochen.

Abschließend wird der Nachteil, dass die Verschlüsselung von großen Datenmengen mit einem asymmetrischen Verfahren sehr aufwändig ist, genannt und das Hybridverfahren kurz angesprochen.

Hintergründe/Bemerkungen:
Die Schüler sollen zuerst einen Überblick darüber bekommen, wie das RSA-Verfahren funktioniert. Bevor das Verfahren im Detail behandelt werden kann, müssen der Euklidische Algorithmus, das Lemma von Bézout und der erweiterte Euklidische Algorithmus eingeführt werden.

Damit die Schüler nachvollziehen können, warum mit dem Euklidischen Algorithmus der größte gemeinsame Teiler berechnet werden kann, sollte zuerst die einfache Variante mit der Differenz und erst dann die Variante mit der Division mit Rest eingeführt werden. Bevor der Algorithmus eingeführt wird, sollte diese zuvor durch ein Beispiel veranschaulicht werden.

Bei der Schlüsselerzeugung ist es nicht zwingend notwendig, das multiplikative Inverse im Restklassenkörper einzuführen. Es genügt, wenn die Schüler mit dem erweiterten Euklidischen Algorithmus ganze Zahlen d und v mit $de + vm = 1$ berechnen. Die Zahl d ist dann der geheime Schlüssel. Je nach Schülerniveau und vorhandener Zeit kann natürlich auch das Inverse Element zuvor eingeführt werden.

Der Beweis, dass man nach dem Entschlüsseln wieder die ursprüngliche Nachricht erhält, ist ein bisschen aufwändig, da zuvor der kleine Satz von Fermat eingeführt und bewiesen werden sollte. Es sollte genügen, den Schülern mit einigen Beispielen nahe zu legen, dass nach Anwenden der Entschlüsselung auf die verschlüsselte Nachricht wieder die ursprüngliche Nachricht erhalten wird. Man kann den Schülern auch mitteilen, dass dies auch bewiesen werden kann, jedoch für die Schulmathematik nicht ganz trivial ist.

Damit die Schüler nicht den Eindruck bekommen, dass asymmetrische Verfahren keine Nachteile mit sich bringen, sollte auf jeden Fall erklärt werden, dass asymmetrische Algorithmen sehr viel langsamer arbeiten als Symmetrische.

Online-Tools *(Stand 1. August 2019):*
Erweiterter Euklidischer Algorithmus:

- `https://www.arndt-bruenner.de/mathe/scripts/erweitertereuklid.htm`
- `http://public.hochschule-trier.de/~knorr/exeuclid.php?a=101&b=35&submit=Berechnen`

Schlüsselerzeugung und Ver- und Entschlüsselung von ganzen Zahlen:

- https://www.cryptool.org/de/cto-highlights/rsa-schritt-fuer-schritt

3.3 Anhang

Arbeitsblatt 1: Skytale

Aufgabe 1: Knacke die Geheimbotschaft!

Herzlich Willkommen beim großen Entschlüsselungs-Wettbewerb. Wir suchen heute Österreichs bestes Codeknacker-Team! Ihr habt es mit starker Konkurrenz zu tun! Es gewinnt das Team, das am schnellsten die fünf Botschaften auf den Papierstreifen, die ihr erhält, in sinnvolle Sätze umwandeln kann.

Als Hilfsmittel benötigt ihr lediglich die drei vorbereiteten Stäbe.

Auf die Plätze, fertig, los!

Aufgabe 2: Nachrichten ver- und entschlüsseln

a) Versuche verschiedene Nachrichten mit den Stäben zu verschlüsseln und lass deine Gruppenmitglieder diese geheimen Nachrichten entschlüsseln.

   Als Hilfsmittel stehen leere Papierstreifen zur Verfügung.

b) Welche Information benötigt der Empfänger, um die geheime Nachricht richtig zu entschlüsseln?

Aufgabe 3: Ver- und Entschlüsseln ohne Skytale

a) Wie kann eine Nachricht nun auf dieselbe Variante ver- bzw. entschlüsselt werden, wenn kein Stab vorhanden ist, um den man den Papierstreifen wickeln kann?

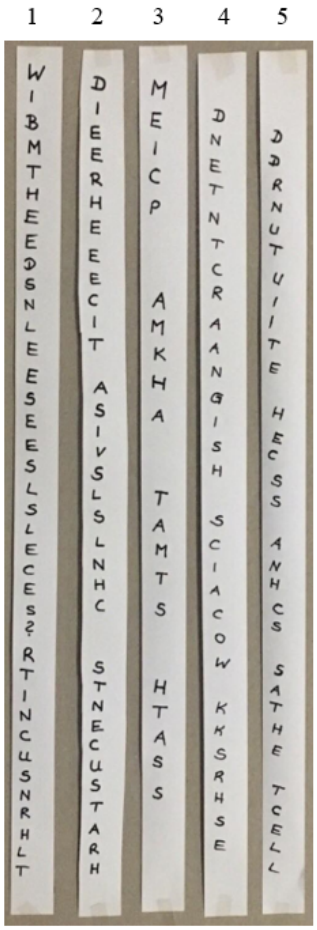
b) Welche Information benötigt nun der Empfänger, um die geheime Nachricht zu entschlüsseln.

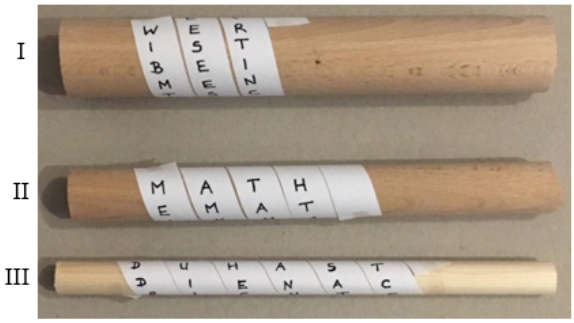
c) Kann der Empfänger die geheime Nachricht entschlüsseln, auch wenn er diese Information nicht hat? Wenn ja, wie?

Aufgabe 4: Internetrecherche

Wann und von wem wurde die Skytale erstmals eingesetzt?

Holzstäbe und Geheimtexte





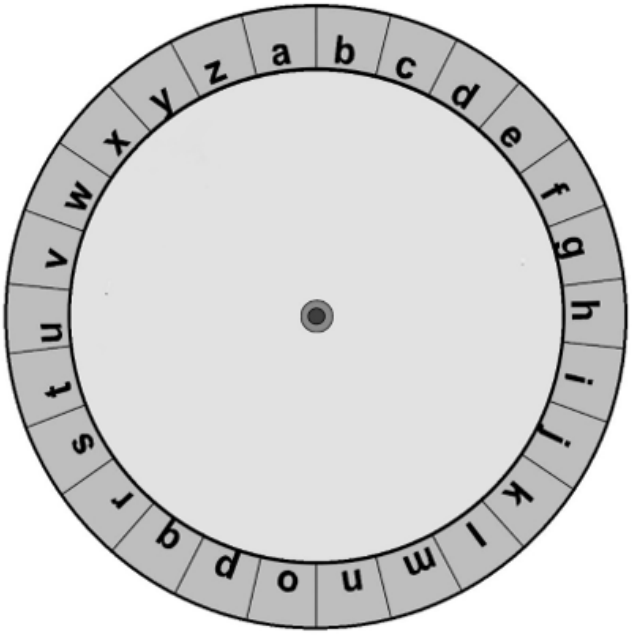
Umfang/Durchmesser der Holzstäbe:

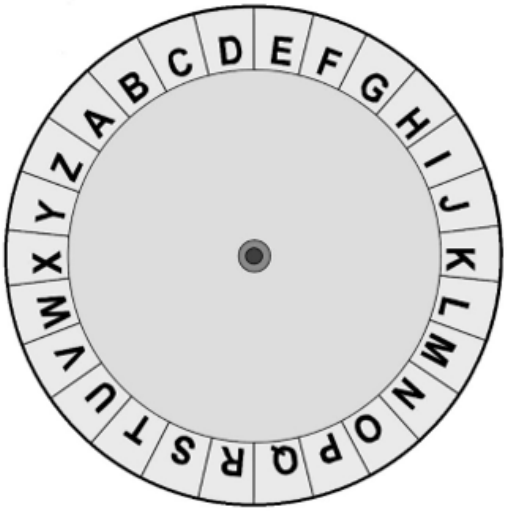
I. 96 mm/30 mm
II. 66 mm/20 mm
III. 43 mm/13 mm

Lösung

1. Geheimtext: *Schlüssel:* Skytale I
Klartext: WER IST BEIM ENTSCHLUESSELN DER SCHNELLSTE?
2. Geheimtext: *Schlüssel:* Skytale I
Klartext: DAS IST EINE VERSCHLUESSELTE NACHRICHT
3. Geheimtext: *Schlüssel:* Skytale II
Klartext: MATHEMATIK MACHT SPASS
4. Geheimtext: *Schlüssel:* Skytale II
Klartext: DAS KNACKEN IST GAR NICHT SO SCHWER
5. Geheimtext: *Schlüssel:* Skytale III
Klartext: DU HAST DIE NACHRICHT ENTSCHLUESSELT

Vorlage: Chiffrierscheibe[10]





Anleitung zum Basteln einer Caesar-Scheibe:

- Klebe die Scheiben auf einen stabilen Karton.
- Schneide beide Scheiben aus.
- Lege die kleinere auf die größere Scheibe und befestige sie mit einer Musterklammer.

[10] Die Vorlage wurde aus Beutelspacher (2009) entnommen und bearbeitet.

Arbeitsblatt 2: Häufigkeitsanalyse

Du hast folgenden Geheimtext, welcher mit einer Caesar-Verschiebung verschlüsselt wurde, abgefangen. Versuche diesen mit der Häufigkeitsanalyse zu brechen!

```
WXK GTFX WXK VTXLTK-OXKLVAENXLLXENGZ EXBMXM LBVA OHF KHXFBLVAXG
YXEWAXKKG ZTBNL CNEBNL VTXLTK TU, WXK GTVA WXK NXUXKEBXYXKNGZ WXL
KHXFBLVAXG LVAKBYMLMXEEXKL LNXMHG WBXLX TKM WXK ZXAXBFXG DHFFNGBDTMB-
HG YÜK LXBGX FBEBMTXKBLVAX DHKKXLIHGWXGS OXKPXGWXM ATM. WTUXB UX-
GNMSMX VTXLTK XBGX OXKLVABXUNGZ WXL TEIATUXML NF WKXB UNVALMTUXG.
```

Lösung
Häufigster Buchstabe: X
Schlüssel: T=19
Klartext:
Der Name der Caesar-Verschluesselung leitet sich vom roemischen Feldherrn Gaius Julius Caesar ab, der nach der Ueberlieferung des roemischen Schriftstellers Sueton diese Art der geheimen Kommunikation für seine militaerische Korrespondenz verwendet hat. Dabei benutzte Caesar eine Verschiebung des Alphabets um drei Buchstaben.[11]

[11] Der Text stammt aus `https://de.wikipedia.org/wiki/Caesar-Verschlüsselung` (Stand 29. Juli 2019)

Arbeitsblatt 3: Knacken der Vigenère-Verschlüsselung

Aufgabe 1:

Du hast den folgenden Geheimtext abgefangen. Du weißt, dass die Nachricht mit der Vigenère-Verschlüsselung chiffriert wurde und das Schlüsselwort aus 7 Buchstaben besteht. Ermittle das Schlüsselwort und entschlüssle den Geheimtext!

```
XZIFBFRSVM VZKRTVLGUL NTKPCLWFUJ MEOIVOXIJL MZUVBVDIYD YITTMGEVVX
PKROVVGCIE TTLNBIFTVP WUKIFIWEOP HFJWGSXJVI HGZIUSCIKJ LGCIIEOIAX
VRPTEAXVMC BWJJVZKLPR OSYEOWGBSI PKEFWVVYLR QFKIUJLYVV WULPJPIXDL
WGFYXYHWVT KEDLVJFERO HRQJVPCLRT FUIUZGUMLI UZIYXFVVZR VDYXMLRAUX
MDAIFWZINS IVDYXGPRRN VXJVHRNZXF LVZBEHKLWP ICYGZWRMNS TAPNFEKGII
FUZQOLRXBE R
```

Aufgabe 2:

Du hast die folgende geheime Botschaft abgefangen und weißt, dass sie mit der Vigenère-Verschlüsselung chiffriert wurde. Bestimme mit dem Kasiski-Test die Schlüsselwortlänge!

```
FOVWUJZXIK USOAGTHGMW PHQMUJHQYJ FOCYVGBNPS THHBLKBGIF ISKIAOHHBL
WACYOCBGID POXGZFSUIE RTDIFISUFJ CIFLLGGXQV GBJIZGWPXW ZHZMWFSUMF
FSQODCFWIP VNXYWDSUWW VNHROGBQAA TOOWGFOVWU JZXIKUSOAG THDYKHWQHA
IADGZGBNSW PBWIFYOHVW GGHMFNSLGZ VSVHWPHHBL BIHRLBWIJW TB
```

Lösung Aufgabe 1

Schlüsselwort: BRECHEN

1. Teiltext: `XSTTUOUDEOTTFFVSCXXJOBWFVPFTFJFMXDUWDNNBIMFUB`
2. Teiltext: `ZVVKJXVYVVTVIJICIVVVSSVKVIYKEVULFYXZYVZECNEZE`
3. Teiltext: `IMLPMIBIVVLPWWHIIRMZYIVIWXXERPIIVXMIXXXHYSKQR`
4. Teiltext: `FVGCEJVTXGNWEGGKEPCKEPYUUDYDOCUUVMDNGJFKGTGO`
5. Teiltext: `BZULOLDTPCBUOSZJOTBLOKLJLLHLHLZZZLASPVLLZAIL`
6. Teiltext: `FKLWIMIMKIIKPXILIEWPWERLPWWVRRGIRRIIRHVWWPIR`
7. Teiltext: `RRNFVZYGREFIHJUGAAJRGFQYJGVJQTUYVAFVRRZPRNFX`

Teiltext	Häufigster Buchstabe	Schlüsselwortbuchstabe
1.	F $\rightarrow$ e	B
2.	V $\rightarrow$ e	R
3.	I $\rightarrow$ e	E
4.	G $\rightarrow$ e	C
4.	L $\rightarrow$ e	H
4.	I $\rightarrow$ e	E
5.	R $\rightarrow$ e	N

Klartext:

Wie du bereits gesehen hast, laesst sich ein Geheimtext, welcher mit der Vigenere-Verschluesselung verschluesselt wurde, sehr leicht brechen, wenn man weiß, aus wie vielen Buchstaben das verwendete Schluesselwort besteht. Was ist aber, wenn man die Laenge des Schluesselworts nicht kennt? Gibt es vielleicht eine Methode, mit der man die Schluesselwortlaenge bestimmen kann?

Lösung Aufgabe 2

Buchstabenwiederholungen:

FOVWUJZXIK USOAGTHGMW PHQMUJHQYJ FOCYVGBNPS THHBLKBGIF ISKIAOHHBL
WACYOCBGID POXGZFSUIE RTDIFISUFJ CIFLLGGXQV GBJIZGWPXW ZHZMWFSUMF
FSQODCFWIP VNXYWDSUWW VNHROGBQAA TOOWGFOVWU JZXIKUSOAG THDYKHWQHA
IADGZGBNSW PBWIFYOHVW GGHMFNSLGZ VSVHWPHHBL BIHRLBWIJW TB

Buchstabenfolge	Abstand
FOVWUJZXIKUSOAGTH	155
IFIS	35
HHBL	15, 160 und 175

Schlüsselwortlänge: $ggT(15, 35, 155, 160, 175) = 5$

Schlüsselwort: CODES

1. Teiltext: FJUTPJFGTKIOWCPFRICGGGZFFCVDVGTFJUTHIGPYGNVPBBT
2. Teiltext: OZSHHHOBHBSHABOSTSIGBWHSSFNSNBOOZSHWABBOGSSHIWB
3. Teiltext: VXOGQQCNHGKHCGXUDUFXJPZUQWXUHQOVXODQDNWHHLVHHI
4. Teiltext: WIAMMYYPBIIBYIGIIFLQIXMMOIYWRAWWIAYHGSIVMGHBRJ
5. Teiltext: UKGWUJVSLFALODZEFJLVZWWFDPWWOAGUKGKAZWFWFZWLLW

Teiltext	Häufigster Buchstabe	Schlüsselwortbuchstabe
1.	G → e	C
2.	S → e	O
3.	H → e	D
4.	I → e	E
5.	W → e	S

Klartext:

„Das Schlüsselwort dient nicht nur dazu, den Klartext in den Geheimtext zu verwandeln, auch der Empfänger braucht es, um den Geheimtext wieder in den Klartext zu übersetzen. Wenn wir also das Schlüsselwort ausfindig machen können, wäre es ein leichtes, den Text zu entziffern."[12]

[12] Singh (2002), S. 80

ASCII-Tabelle

ASCII-TABELLE								
Zeichen	Binär	Dez.	Zeichen	Binär	Dez.	Zeichen	Binär	Dez.
[Leerzeichen]	0010 0000	32	@	0100 0000	64	`	0110 0000	96
!	0010 0001	33	A	0100 0001	65	a	0110 0001	97
"	0010 0010	34	B	0100 0010	66	b	0110 0010	98
#	0010 0011	35	C	0100 0011	67	c	0110 0011	99
$	0010 0100	36	D	0100 0100	68	d	0110 0100	100
%	0010 0101	37	E	0100 0101	69	e	0110 0101	101
&	0010 0110	38	F	0100 0110	70	f	0110 0110	102
'	0010 0111	39	G	0100 0111	71	g	0110 0111	103
(	0010 1000	40	H	0100 1000	72	h	0110 1000	104
)	0010 1001	41	I	0100 1001	73	i	0110 1001	105
*	0010 1010	42	J	0100 1010	74	j	0110 1010	106
+	0010 1011	43	K	0100 1011	75	k	0110 1011	107
,	0010 1100	44	L	0100 1100	76	l	0110 1100	108
-	0010 1101	45	M	0100 1101	77	m	0110 1101	109
.	0010 1110	46	N	0100 1110	78	n	0110 1110	110
/	0010 1111	47	O	0100 1111	79	o	0110 1111	111
0	0011 0000	48	P	0101 0000	80	p	0111 0000	112
1	0011 0001	49	Q	0101 0001	81	q	0111 0001	113
2	0011 0010	50	R	0101 0010	82	r	0111 0010	114
3	0011 0011	51	S	0101 0011	83	s	0111 0011	115
4	0011 0100	52	T	0101 0100	84	t	0111 0100	116
5	0011 0101	53	U	0101 0101	85	u	0111 0101	117
6	0011 0110	54	V	0101 0110	86	v	0111 0110	118
7	0011 0111	55	W	0101 0111	87	w	0111 0111	119
8	0011 1000	56	X	0101 1000	88	x	0111 1000	120
9	0011 1001	57	Y	0101 1001	89	y	0111 1001	121
:	0011 1010	58	Z	0101 1010	90	z	0111 1010	122
;	0011 1011	59	[	0101 1011	91	{	0111 1011	123
<	0011 1100	60	\	0101 1100	92	|	0111 1100	124
=	0011 1101	61	]	0101 1101	93	}	0111 1101	125
>	0011 1110	62	^	0101 1110	94	~	0111 1110	126
?	0011 1111	63	–	0101 1111	95			

Abbildung 9: ASCII-Tabelle[13]

[12]Gómez (2016), S. 78

Literaturverzeichnis

Bauer, F. L. (1997). *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie*, 2. erweiterte Auflage, Springer Berlin Heidelberg.

Beutelspacher, A. (2002). *Geheimsprachen: Geschichte und Techniken*, 3. aktualisierte Auflage, Verlag C. H. Beck oHG, München.

Beutelspacher, A. (2009). *Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen*, 9. Auflage, Vieweg+Teubner | GWV Fachverlage GmbH, Wiesbaden.

Beutelspacher, A., Neumann, B. H. und Scharzpaul, T. (2010). *Kryptografie in Theorie und Praxis: Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld*, 2. überarbeitete Auflage., Vieweg+Teubner | GWV Fachverlage GmbH, Wiesbaden.

Beutelspacher, A. und Zschiegner, M.-A. (2011). *Diskrete Mathematik für Einsteiger: Mit Anwendungen in Technik und Informatik*, 4. aktualisierte Auflage, Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH.

Borys, T. (2011). *Codierung und Kryptologie: Facetten einer anwendungsorientierten Mathematik im Bildungsprozess*, Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH.

Ertel, W. (2012). *Angewandte Kryptographie*, 4. überarbeitete und ergänzte Auflage, Carl Hanser Verlag München.

Freiermuth, K., Hromkovič, J., Keller, L. und Steffen, B. (2010). *Einführung in die Kryp-*

tologie: Lehrbuch für Unterricht und Selbststudium, 2. überarbeitete Auflage, Springer Vieweg, Wiesbaden.

Gómez, J. (2016). *Geheimsprachen und Decodierung: Mathematiker, Spione und Hacker*, Librero.

Horster, P. (1985). *Kryptologie*, Reihe Informatik, Band 47, Mannheim; Wien; Zürich: Bibliogaphisches Institut.

Karpfinger, C. und Kiechle, H. (2010). *Kryptologie: Algebraische Methoden und Algorithmen*, Vieweg+Teubner | GWV Fachverlage GmbH, Wiesbaden.

Rempe, L. und Waldecker, R. (2009). *Primzahltests für Einsteiger: Zahlentheorie – Algorithmik – Kryptographie*, Vieweg+Teubner | GWV Fachverlage GmbH, Wiesbaden.

RIS (2011). Lehrpläne - Höhere technische und gewerbliche Lehranstalten, `https://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20007451/Lehrpläne der Höheren technischen und gewerblichen Lehranstalten %2c Fassung vom 01.08.2019.pdf`. Stand 1. August 2019.

RIS (2018). Lehrpläne - Neue Mittelschule, `https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40207228/NOR40207228.pdf`. Stand 1. August 2019.

RIS (2019). Lehrpläne - Allgemeinbildende höhere Schulen, `https://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/10008568/Lehrpläne - allgemeinbildende höhere Schulen%2c Fassung vom 01.08.2019.pdf`. Stand 1. August 2019.

Schwenk, J. (2014). *Sicherheit und Kryptographie im Internet: Theorie und Praxis*, 4. überarbeitete u. erweiterte Auflage, Springer Fachmedien Wiesbaden.

Singh, S. (2002). *Codes: Die Kunst der Verschlüsselung*, Carl Hanser Verlag München.

Spitz, S., Pramateftakis, M. und Joachim, S. (2011). *Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen*, 2. überarbeitete Auflage, Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH.

Wätjen, D. (2018). *Kryptographie: Grundlagen, Algorithmen, Protokolle*, 3. Auflage, Springer Fachmedien Wiesbaden GmbH.

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides statt durch meine eigenhändige Unterschrift, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe. Alle Stellen, die wörtlich oder inhaltlich den angegebenen Quellen entnommen wurden, sind als solche kenntlich gemacht.

Die vorliegende Arbeit wurde bisher in gleicher oder ähnlicher Form noch nicht als Magister-/Master-/Diplomarbeit/Dissertation eingereicht.

Datum	Unterschrift