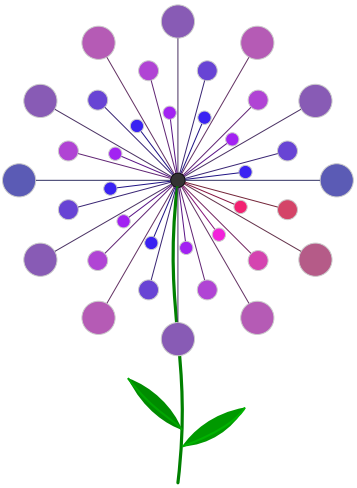


FreeFlower

Informatik

Kryptologie

Skript

Inhaltsverzeichnis

Kapitel 1

Geheimschriften und einfache Kryptosysteme

1.1 Einführung

Alice möchte Bob eine vertrauliche Nachricht (z. B. Bankdaten, gesundheitliche Befunde) über das Internet zukommen lassen. Nun ist das Internet ein sehr grosses physisches Netzwerk, das sich über die ganze Welt erstreckt. Es besteht aus unzähligen Kabeln, Routern, Servern, etc., die von verschiedenen Organisationen und Staaten betrieben werden. Wenn Alice eine Nachricht an Bob sendet, wird diese Nachricht über dieses Netzwerk transportiert und durchläuft dabei viele verschiedene Geräte und Verbindungsstrecken. Es ist für Alice und Bob, praktisch gesprochen, unmöglich auszuschliessen, dass jemand die Nachricht mitlesen / mithören könnte, während sie über das Internet transportiert wird.

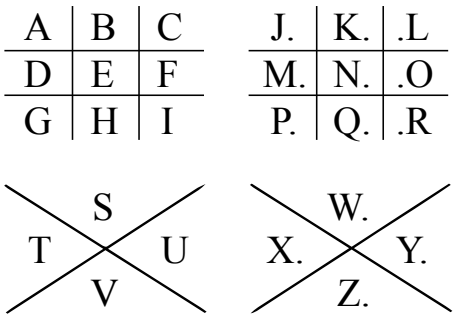
Die *Kryptologie* befasst sich (unter anderem) mit der Frage, wie Alice ihre ursprüngliche Nachricht (*Klartext*) vor der Übertragung so verändern kann, dass es nur für den vorgesehenen Empfänger Bob, jedoch nicht für einen unbefugten Angreifer, möglich ist, aus der veränderten Nachricht den Klartext zu rekonstruieren. Der Angreifer würde im Idealfall also lediglich einen unverständlichen „Wortsalat“ mitlesen, der für ihn unverständlich ist.

1.2 Geheimschriften

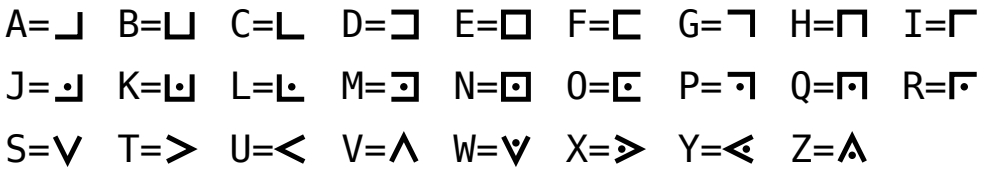
Sicherlich haben Sie als Kind schon einmal eine Geheimschrift erfunden, um geheime Nachrichten mit Ihren Freunden auszutauschen.

Beispiel 1.1 (Geheimschrift der Freimaurer)**:**
Recht bekannt ist das *Freimaurer-Alphabet*. Bei dieser Geheimschrift werden die lateinischen Grossbuchstaben des Klartexts durch neue Symbole ersetzt. Die Sicherheit dieses Verfahrens beruht allein darauf, dass die Regeln der Übersetzung geheim gehalten werden (*Security through Obscurity*). In Abbildung 1.1 sehen Sie, wie die Geheimschrift der Freimaurer aufgebaut ist und wie die Symbole den Buchstaben zugeordnet werden.

Dem Buchstaben `A` im Klartext wird zum Beispiel das Symbol ⌟ zugeordnet, dem Buchstaben `B` das Symbol ⌴, dem Buchstaben `C` das Symbol ⌞, und so weiter. So wird zum Beispiel aus dem Klartext `HALLO` der Geheimtext ⊓⌟⊢⊢⊏.



(a) Freimaurer-Alphabet



(b) Zuordnung der Symbole zu den lateinischen Grossbuchstaben

Abbildung 1.1: Freimaurer-Geheimschrift: Beispiel für ein Verfahren, dessen Sicherheit von der Geheimhaltung des Systems abhängt.
Quelle: Wikimedia Commons

Das allgemeine Schema der Verwendung einer Geheimschrift ist in Abbildung 1.2 dargestellt. Alice (Sender) *chiffriert* den Klartext, um den Geheimtext zu erhalten, und übermittelt diesen über einen unsicheren Kanal (z. B. Internet, Telefonie) an Bob (Empfänger). Bob *dechiffriert* den Geheimtext, um wieder den Klartext zu erhalten. Ein Angreifer (Eve) könnte versuchen, den Geheimtext abzufangen und zu dechiffrieren, um den Klartext zu erfahren.

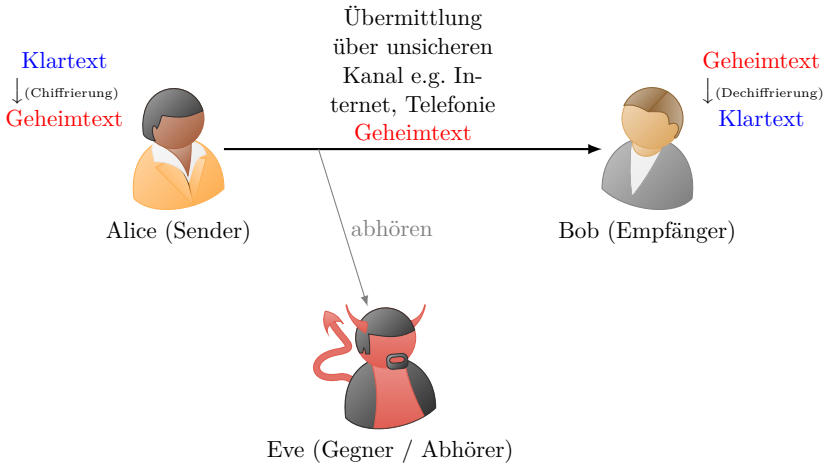


Abbildung 1.2: Dieses Schema zeigt die Kommunikation zwischen Alice (Sender) und Bob (Empfänger) unter Verwendung einer Geheimschrift. Der Name *Eve* ist eine clevere Abkürzung für *eavesdropper*, was auf Deutsch so viel wie *Abhörer* bedeutet.

Definition 1.1 (Geheimschrift)**:**
Eine **Geheimschrift** realisiert eine Transformation (*Chiffrierung*) von einem Klartext in

einen Geheimtext. Die Umkehrung dieser Transformation (*Dechiffrierung*) ermöglicht es, den Klartext aus dem Geheimtext (typischerweise eindeutig) zu rekonstruieren:

$$\text{Chiffrierung}(\text{Klartext}) = \text{Geheimtext}$$
$$\text{Dechiffrierung}(\text{Geheimtext}) = \text{Klartext}.$$

Beispielsweise:

$$\text{Freimaurer\_Chiffrierung}(\texttt{HALLO}) = \square\lrcorner\llcorner\llcorner\square$$
$$\text{Freimaurer\_Dechiffrierung}(\square\lrcorner\llcorner\llcorner\square) = \texttt{HALLO}.$$

1.3 Von Geheimschriften zu Kryptosystemen

Geheimschriften haben eine lange Geschichte und wurden in verschiedenen Kulturen und Epochen verwendet, um geheime Nachrichten zu übermitteln. Sie sind ein wichtiger Bestandteil der Kryptologie, da sie die Grundlage für die Entwicklung der modernen Kryptoverfahren bilden. Die Verwendung von Geheimschriften hat aber einen entscheidenden Nachteil: Wenn die Regeln der Geheimschrift bekannt werden, kann jeder, der den Geheimtext abfängt, diesen dechiffrieren und den Klartext lesen. Daher sind Geheimschriften allein nicht ausreichend, um die Vertraulichkeit von Nachrichten zu gewährleisten, insbesondere in einer Welt, in der Informationen leicht zugänglich und verbreitet werden können.

Bemerkung 1.1 (*Security through Obscurity*)**:**
Security through Obscurity (Sicherheit durch Verschleierung) bezeichnet die Praxis, die Sicherheit eines Systems dadurch zu gewährleisten, dass die Funktionsweise des Systems geheim gehalten wird. Die Praxis der *Security through Obscurity* wird als unsicher angesehen, da sie auf der Annahme beruht, dass Angreifer nicht in der Lage sein werden, die Funktionsweise des Systems zu verstehen oder zu entdecken.

Idee 1.1 (Kryptosystem)**:**
Wir wollen von Geheimschriften zu sogenannten **Kryptosystemen** übergehen, die so konstruiert sind, dass sie auch dann sicher sind, wenn die grundlegende Funktionsweise des Systems öffentlich bekannt ist.

Ein solches System kennen Sie bereits aus dem Alltag: Wir wissen alle, wie ein Türschloss grundsätzlich mit einem Schlüssel zu öffnen ist, aber dennoch können wir unsere Türen sicher verschliessen, da die Sicherheit nicht von der Geheimhaltung des Mechanismus abhängt, sondern von der Geheimhaltung (sicheren Aufbewahrung) des Schlüssels.

Wir werden im Folgenden einige einfache Kryptosysteme kennenlernen, um zu verstehen, was ein sicheres Kryptosystem auszeichnet.

1.4 Beispiele einfacher Kryptosysteme

1.4.1 Das Kryptosystem *Skytale*

Das bereits von den Griechen für militärische Zwecke verwendete Kryptosystem *Skytale* basiert auf der **Transposition**: Dabei bleiben die Buchstaben des Klartexts im Kryptotext zwar erhalten, ändern aber nach folgendem Algorithmus ihre Positionen:

- Schreibe den Klartext zeilenweise in eine Tabelle (Matrix) von links nach rechts.
- Allfällige leere Felder in der letzten Zeile der Tabelle werden mit beliebigen (am besten zufällig gewählten) Buchstaben gefüllt.
- Den Kryptotext erhalten wir, indem wir die Buchstaben Spalte für Spalte von links nach rechts und von oben nach unten lesen.

Die Skytale wird mit einem Stab und einem Band umgesetzt (Abbildung 1.3). Die Anzahl der Zeichen pro Windung entspricht dabei der Zeilenanzahl der Tabelle und bildet somit den Schlüssel.

Abbildung 1.3: Praktische Umsetzung der Skytale-Verschlüsselung mit einem Stab und einem Band. Die Anzahl Zeichen, die auf eine Windung des Bandes um den Stab passen, entspricht der Anzahl Zeilen in der Tabelle, also dem Schlüssel des Kryptosystems *Skytale*.
Quelle: Wikimedia Commons

Aufgabe 1.1

Der Kryptotext

`WNGIAEIEMATSMKRTTEAGIEINANINTUGNDOJEEENL`

wurde mit einer Tabelle mit 5 Zeilen und 8 Spalten erzeugt. Wie lautet der Klartext? Tipp: Nehmen Sie Ihr bevorzugtes Tabellenkalkulationsprogramm zuhilfe oder verwenden Sie diesen Link mit *Analysewerkzeug* → *Tabelle*.

Aufgabe 1.2

Der folgende Kryptotext der Länge 35 wurde mit Skytale verschlüsselt:

`SRESIENITEIINHFNCDIROHAEADTSRGESIDE`

Dabei konnten mit dem Klartext **alle Zeilen der Tabelle vollständig aufgefüllt** werden.

1. Wie viele verschiedene Schlüssel (Anzahl Zeilen) sind in dieser Situation möglich?
2. Welcher Schlüssel wurde hier verwendet? Tipp: Sie können diesen Link mit *Analysewerkzeug* → *Tabelle* dazu verwenden.
3. Wie lautet der Klartext?

Aufgabe 1.3

Sie möchten einen Klartext der Länge 87 mit Hilfe einer Tabelle mit 10 Zeilen verschlüsseln. Wie viele Spalten benötigt diese Tabelle?

Aufgabe 1.4

Wie die Skytale, beruht auch die folgende Verschlüsselungsmethode auf der Transposition von Buchstaben. Finden Sie zu den folgenden Kryptotexten die Klartexte (unverschlüsselte Nachrichten):

1. `RKPYOTOLIGEEMREOLGCITHEGEHMIINSSE`
2. `HCSFIRILTAHCZFUEBUHAWNERDNUKUZMMOINUEIZNER`

1.4.2 Das Kryptosystem *Caesar*

Eines der bekanntesten Kryptosysteme der Antike ist die Caesar-Verschlüsselung, die von Julius Caesar verwendet wurde. Dabei wird jeder Buchstabe des Klartexts um eine feste Anzahl von Positionen im Alphabet verschoben. Die Anzahl der Positionen, um die verschoben wird, bildet den Schlüssel des Kryptosystems.

Bemerkung 1.2 (Buchstaben als Zahlen)**:**
Häufig wird die Verschiebung nicht direkt als Zahl angegeben, sondern als Buchstabe, der die Anzahl der Positionen angibt. So steht beispielsweise der Schlüssel `A` für eine Verschiebung um 0 Positionen (keine Verschiebung), `B` für eine Verschiebung um 1 Position, `C` für eine Verschiebung um 2 Positionen, `D` für eine Verschiebung um 3 Positionen und so weiter:

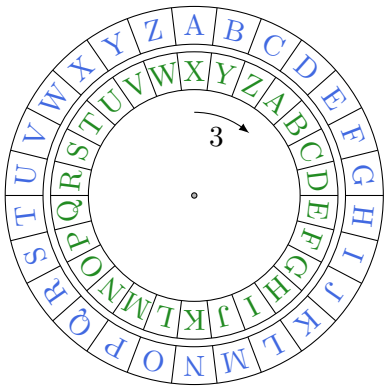
`A` ↔ 0 Positionen, `B` ↔ 1 Position, `C` ↔ 2 Positionen, ..., `Z` ↔ 25 Positionen.

Definition 1.2 (Ordnung eines Buchstabens)**:**
Die **Ordnung** eines Buchstabens ist die Anzahl der Positionen, die dieser Buchstabe im Alphabet von `A` entfernt ist. Wir definieren

$$\mathrm{Ord}(\texttt{A}) = 0,\ \mathrm{Ord}(\texttt{B}) = 1,\ \mathrm{Ord}(\texttt{C}) = 2,\ \ldots,\ \mathrm{Ord}(\texttt{Z}) = 25.$$

Beispiel 1.2 (Caesar mit Schlüssel `D`)**:**
Mit dem Schlüssel `D` (3 Positionen, da $\mathrm{Ord}(\texttt{D}) = 3$) wird aus dem Klartext `HALLO` der Kryp-

totext `KDOOR`:



Dabei haben wir die innere Scheibe um 3 Positionen im Uhrzeigersinn gedreht, um die Verschlüsselung durchzuführen („lesen von innen nach aussen“). Zur Entschlüsselung

- lesen wir die Drehscheiben, genau so wie sie in Beispiel 1.2 angeordnet sind, von „aussen nach innen“
- oder drehen die innere Scheibe um 3 Positionen gegen den Uhrzeigersinn zurück in die Ausgangsposition (`A` ↔ `A`) und dann nochmals um 3 Positionen gegen den Uhrzeigersinn (dies können wir um eine Verschiebung um -3 Positionen anschauen). Mit diesem Vorgehen können wir die Drehscheiben wieder von „innen nach aussen“ lesen, um den Klartext zu erhalten.

Hier finden Sie ein interaktives Werkzeug, um die Caesar-Verschlüsselung und -Entschlüsselung durchzuführen.

Beispiel 1.3:
Folgender Text wurde mit dem Schlüssel `G` (6 Positionen) verschlüsselt:

```
Klartext:   JEMANDMUSSTEJOSEFVERLEUMDETHA...
Schlüssel:  GGGGGGGGGGGGGGGGGGGGGGGGGGG...
Kryptotext: PKSGTJSAYYZKPUYKLBKXRKASJKZNG...
```

Aufgabe 1.5

Der Kryptotext

`X G T Y G P F G U E J N W G U U G N B Y G K`

wurde mit Caesar verschlüsselt, der Schlüssel ist aber unbekannt. Entschlüsseln Sie den Kryptotext, ohne alle Schlüssel auszuprobieren, wenn Sie wissen, dass der häufigste Buchstabe im Klartext `E` ist. Verwenden Sie das interaktive Werkzeug, um die Entschlüsselung durchzuführen.

1.5 Allgemeine Betrachtungen zu Kryptosystemen

1.5.1 Definition eines Kryptosystems

Ein Kryptosystem besteht aus einem Verschlüsselungsalgorithmus, einem Entschlüsselungsalgorithmus und einem Schlüssel. Der Verschlüsselungsalgorithmus nimmt den Klartext und den Schlüssel als Eingabe und erzeugt den Kryptotext. Der Entschlüsselungsalgorithmus nimmt den Kryptotext und den Schlüssel als Eingabe und rekonstruiert den Klartext. Die Sicherheit eines Kryptosystems sollte nicht davon abhängen, dass die Funktionsweise des Systems geheim gehalten wird, sondern allein von der Geheimhaltung des Schlüssels.

Das Schema in Abbildung 1.5 zeigt die Kommunikation zwischen Alice (Sender) und Bob (Empfänger) unter Verwendung eines Kryptosystems. Alice verschlüsselt den Klartext mit dem Schlüssel, um den Kryptotext zu erhalten, und übermittelt diesen über einen unsicheren Kanal (z. B. Internet, Telefonie) an Bob. Bob benötigt den Schlüssel, um den Kryptotext zu entschlüsseln und den Klartext zu erhalten. Ein Angreifer (Eve) könnte versuchen, den Kryptotext abzufangen und zu entschlüsseln, um den Klartext zu erfahren.

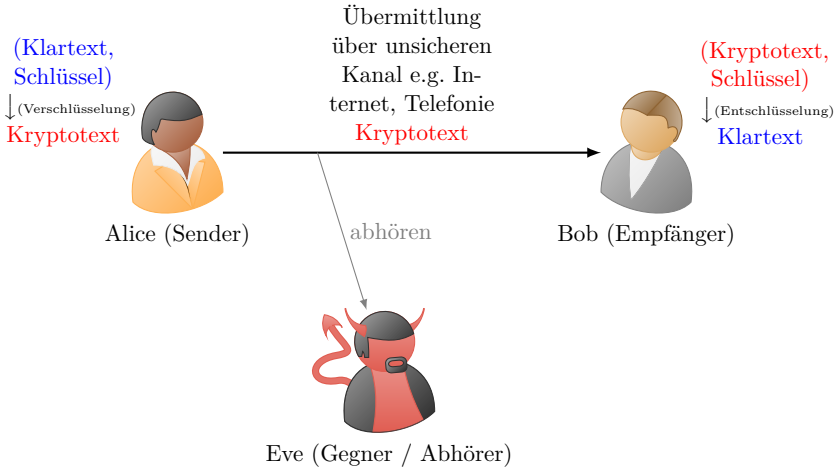


Abbildung 1.5: Kommunikation zwischen Alice (Sender) und Bob (Empfänger) unter Verwendung eines Kryptosystems. Bob benötigt den Schlüssel, um den Kryptotext zu entschlüsseln.

Definition 1.3 (Kryptosystem)**:**
Ein **Kryptosystem** realisiert eine Transformation (*Verschlüsselung*) von einem Klartext in einen Kryptotext, die von einem Schlüssel abhängt. Die Menge aller möglichen Schlüssel wird *Schlüsselmenge* des Kryptosystems genannt. Die Umkehrung dieser Transformation (*Entschlüsselung*) ermöglicht es, den Klartext aus dem Kryptotext zu rekonstruieren, wenn man den Schlüssel kennt:

$$\begin{aligned}\text{Verschlüsselung}(\text{Klartext}, \text{Schlüssel}) &= \text{Kryptotext}\\ \text{Entschlüsselung}(\text{Kryptotext}, \text{Schlüssel}) &= \text{Klartext}.\end{aligned}$$

Beispielsweise (mit Caesar):

$$\begin{aligned}\text{Caesar\_Verschlüsselung}(\texttt{HALLO}, 3) &= \texttt{KDOOR}\\ \text{Caesar\_Entschlüsselung}(\texttt{KDOOR}, 3) &= \texttt{HALLO}.\end{aligned}$$

Schlüsselmenge bei Caesar: $\{0, 1, \ldots, 25\}$ beziehungsweise $\{\text{Ord}(\texttt{A}), \text{Ord}(\texttt{B}), \ldots, \text{Ord}(\texttt{Z})\}$.

Bemerkung 1.3 (Geheimschrift als Spezialfall eines Kryptosystems)**:**
Eine Geheimschrift ist ein Spezialfall eines Kryptosystems, bei dem die Schlüsselmenge nur ein einziges Element enthält, nämlich die Anweisung, wie die Buchstaben vertauscht werden. Umgekehrt, kann ein Kryptosystem als eine Sammlung von Geheimschriften betrachtet werden, wobei für jede mögliche Schlüssel eine Geheimschrift definiert ist, die die Buchstaben entsprechend der Verschlüsselungsregel vertauscht.

1.5.2 Kerckhoffs'sches Prinzip

Der niederländische Kryptologe und Linguist *Auguste Kerckhoffs* stellte im Jahr 1883 die folgende Anforderung an die Sicherheit von Kryptosystemen auf, die heute als **Kerckhoffs'sches Prinzip** bekannt ist:

Zitat 1.1:
„Ein Kryptosystem sollte auch dann sicher sein, wenn alles über das System bekannt ist, ausser dem Schlüssel." – Auguste Kerckhoffs, *La cryptographie militaire* (1883)[a]

[a] Originalzitat: „Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi."

Abbildung 1.6: Auguste Kerckhoffs (1835–1903)

Das Kerckhoffs'sche Prinzip besagt, dass die Sicherheit eines Kryptosystems nicht davon abhängen sollte, dass die Funktionsweise des Systems geheim gehalten wird. Stattdessen sollte die Sicherheit allein auf der Geheimhaltung des Schlüssels beruhen. Einem solchen System wird auch dann noch vertraut, wenn es öffentlich bekannt ist, da die Sicherheit nicht von der Geheimhaltung des Algorithmus abhängt, sondern von der Geheimhaltung des Schlüssels. Demgegenüber steht die Praxis der *Security through Obscurity*, bei der die Sicherheit eines Systems dadurch gewährleistet wird, dass die Funktionsweise des Systems geheim gehalten wird. Diese Praxis wird als unsicher angesehen, da sie auf der Annahme beruht, dass Angreifer nicht in der Lage sein werden, die Funktionsweise des Systems zu verstehen oder zu entdecken (siehe auch Bemerkung 1.1).

1.6 Kryptoanalyse von Caesar

Die Caesar-Verschlüsselung ist ein einfaches Kryptosystem, das leicht zu knacken ist. Es gibt zwei Hauptmethoden, um den Schlüssel zu bestimmen und den Klartext zu rekonstruieren:

- Einerseits reicht es, alle 26 (0 bis 25) möglichen Verschiebungen auszuprobieren. Ein moderner Computer hat dies in einigen Millisekunden erledigt. Natürlich muss ein Angreifer (beziehungsweise sein Computer) auch die Möglichkeit haben, den Klartext zu erkennen, wenn er ihn sieht, z. B. durch die Erkennung von sinnvollen Wortteilen (e.g. Abgleich mit einem deutschen Wörterbuch).
- Andererseits kann, wenn der Text genügend lang ist, anhand der Häufigkeit der verschlüsselten Buchstaben mittels einer sogenannten *Häufigkeitsanalyse* in kürzester Zeit bestimmt werden, was der Schlüssel war (vielleicht erinneren Sie sich noch an Aufgabe 1.5). Abbildung 1.7 zeigt die Häufigkeiten der Buchstaben eines langen, mit Caesar verschlüsselten Texts im Kryptotext.

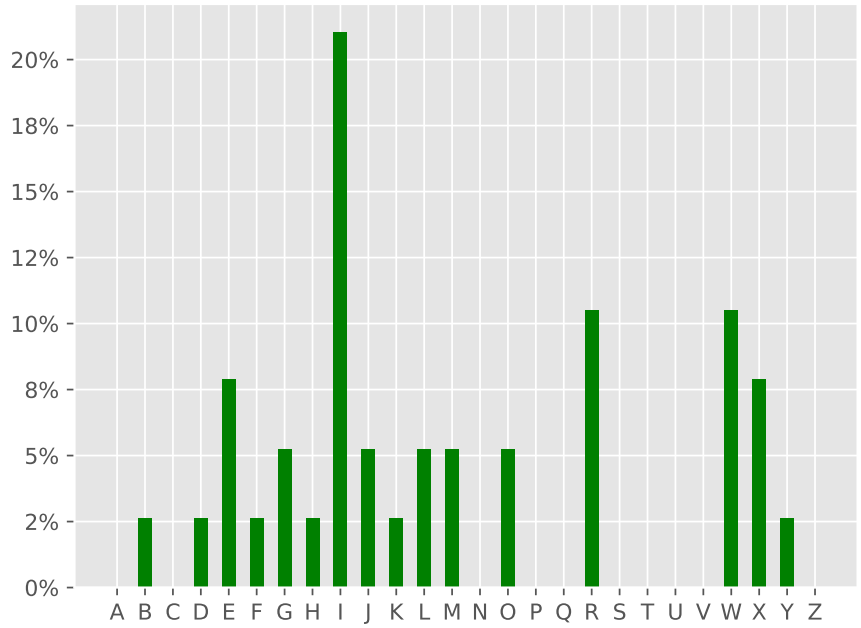


Abbildung 1.7: Buchstabenhäufigkeit in einem nach Caesar verschlüsselten Text

Die durchschnittlichen Häufigkeiten der häufigsten Buchstaben, Bi- und Tri-Grammen in deutschen Texten ist in Tabelle 1.1 angegeben.

Buchstabe	Relative Häufigkeit (%)
E	17.40
N	9.78
I	7.55
S	7.27
R	7.00
A	6.51
T	6.15
D	5.08
H	4.76
U	4.35

(a) Buchstabenhäufigkeit

Bigramm	Relative Häufigkeit (%)
ER	3.94
EN	3.07
CH	2.73
DE	2.41
EI	2.29
ND	2.07
IE	1.97
GE	1.88
TE	1.88
IN	1.82

(b) Bigrammhäufigkeit

Trigramm	Relative Häufigkeit (%)
DER	1.44
SCH	1.21
ICH	1.08
DIE	0.98
UND	0.95
DEN	0.78
CHE	0.77
EIN	0.75
NDE	0.74
GEN	0.72

(c) Trigrammhäufigkeit

Tabelle 1.1: Relative Häufigkeiten der Buchstaben, Bigramme und Trigramme in der deutschen Sprache.

Aufgabe 1.6

Können Sie mit Hilfe einer Häufigkeitsanalyse den Klartext finden? Verwenden Sie Tabelle 1.1, um den Schlüssel zu erraten und den Text zu entschlüsseln.

Kryptotext:

`WMILEFIRIWKIWGLEJJXHMIWIRXIBXDYOREGOIR`

Verwenden Sie das interaktive Werkzeug, um die Entschlüsselung durchzuführen.

Aufgabe 1.7

Kann man immer wie in Aufgabe 1.6 vorgehen? In welchen Fällen funktioniert dieses Vorgehen eventuell nicht?

Aufgabe (Challenge) 1.8

Um zu verschlüsseln, liest man die Caesar-Drehscheiben von innen (Klartext) nach aussen (Kryptotext). Um zu entschlüsseln, liest man von aussen (Kryptotext) nach innen (Klartext). Gibt es Schlüssel bei Caesar, bei denen es sowohl für die Ver- wie Entschlüsselung keine Rolle spielt, in welche Richtung man die Scheiben liest?

1.7 Allgemeine monoalphabetische Substitution

Bei einer *monoalphabetischen Substitution* wird jeder Buchstabe des Klartexts während des gesamten Verschlüsselungsvorgangs nach einer festen Regel durch exakt ein und denselben Kryptotext-Buchstaben ersetzt. Caesar ist ein Spezialfall einer monoalphabetischen Substitution, bei der jeder

Buchstaben im Klartext um dieselbe feste (durch den Caesar-Schlüssel bestimmte) Anzahl Positionen zu verschieben ist.

Im Allgemeinen könnten wir aber auch jede beliebige *Permutation* (Eins-zu-Eins-Zuordnung) von Buchstaben zu erlauben. Eine solche Permutation ist in Abbildung 1.8 dargestellt. Wir nennen dieses Kryptosystem **allgemeine monoalphabetische Substitution**.

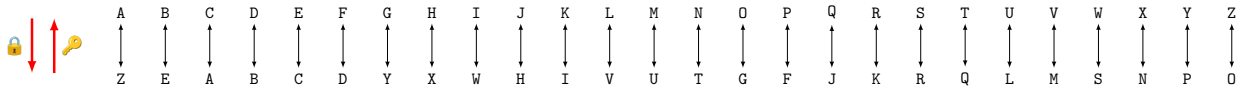


Abbildung 1.8: Monoalphabetische Substitution

Aufgabe 1.9

Wie viele verschiedene Zuordnungsmöglichkeiten (verschiedene Schlüssel) hat die Verschlüsselungsmethode in Abbildung 1.8?

In Aufgabe 1.9 haben Sie gesehen, dass es eine sehr grosse Anzahl solcher Zuordnungen gibt. Obschon die Schlüsselmenge bei der allgemeinen monoalphabetischen Substitution viel grösser ist als bei Caesar, kann dieser Verschlüsselungsalgorithmus ebenfalls (wie Caesar) sehr einfach mit Hilfe einer Häufigkeitsanalyse geknackt werden. Das genauere Vorgehen wird in Beispiel 1.4 illustriert.

Beispiel 1.4:
Folgender Kryptotext wurde abgefangen:

`MUMMUXJUQYMHQOUSUTUQNGWTJQVHUMXQUXQJSUVYPPUM`

Wir wissen, dass er durch eine monoalphabetische Substitution, wie beispielsweise in Abbildung 1.8, entstand, kennen jedoch den Schlüssel (die Zuordnungen der Buchstaben) nicht. Nun verwenden wir Tabelle 1.1, um den Schlüssel zu erraten und den Text zu entschlüsseln. Dabei gehen wir wie folgt vor:

- Wir beginnen damit, die häufigsten Buchstaben zu zählen: `U` kommt 10-mal vor, `M` kommt 6-mal vor und `Q` kommt 6-mal vor. Aufgrund von Tabelle 1.1 versuchen wir, folgendes einzusetzen: `U` ↔ `E`, `M` ↔ `N`, `Q` ↔ `I`. Wir erhalten folgenden Teil-Klartext:
  ```
  KRYPTOTEXT: MUMMUXJUQYMHQOUSUTUQNGWTJQVHUMXQUXQJSUVYPPUM
  KLARTEXT:   NENNE--EI-N-I-E-E-EI-----I--EN-IE-I--E----EN
  ```
  (Die Zuweisung `Q` ↔ `N` anstelle von `M` ↔ `N` scheint uns an dieser Stelle weniger plausibel, da das Wort `ENNEN` im Deutschen nicht existiert, das Wort `NENNEN` jedoch schon.)
- Nun könnten wir weiterfahren, indem wir die häufigsten Trigramme anschauen. Dabei suchen wir im bisherigen Klartext nach Klartext-Teilen, wo wir Trigramme einsetzen könnten. Laut Tabelle 1.1 ist ein häufiges Trigramm in deutschen Texten `DIE`. Dieses probieren wir einzusetzen und vermuten also `D` ↔ `X`:
  ```
  KRYPTOTEXT: MUMMUXJUQYMHQOUSUTUQNGWTJQVHUMXQUXQJSUVYPPUM
  KLARTEXT:   NENNED-EI-N-I-E-E-EI-----I--ENDIEDI--E----EN
  ```
- Der Klartext nimmt langsam Form an und wir können nun damit beginnen, verbleibende Worte zu erraten. Könnte es sich beim ersten Wort um das Wort `DREI` handeln? Wir setzen ein:

```
KRYPTOTEXT: MUMMUXJUQYMHQOUSUTUQNGWTJQVHUMXQUXQJSUVYPPUM
KLARTEXT:   NENNEDREI-N-I-E-E-EI----RI--ENDIEDIR-E----EN
```

- Sobald einzelne Wörter erkannt werden, können wir sie mit Trennlinien voneinander abgrenzen:
```
KRYPTOTEXT: MUMMU|XJUQ|YMHQOUSUTUQNGWTJQVHUM|XQU|XQJ|SUVYPPUM
KLARTEXT:   NENNE|DREI|-N-I-E-E-EI----RI--EN|DIE|DIR|-E----EN
```

- Wir fahren durch Ausprobieren und Erraten weiter, bis das Lösungswort gefunden ist:
```
KRYPTOTEXT: MUMMU|XJUQ|YMHQOU|SUTUQNGWTJQVHUM|XQU|XQJ|SUVYPPUM
KLARTEXT:   NENNE|DREI|ANTIKE|GEHEIMSCHRIFTEN|DIE|DIR|GEFALLEN
```

Je länger ein Text ist, desto zuverlässiger funktioniert das „Erraten“ der Buchstaben per Häufigkeitsanalyse.

Bemerkung 1.4 (Grosse Schlüsselmenge notwendig, aber nicht hinreichend für Sicherheit)**:** Obwohl gemäss Aufgabe 1.9 die monoalphabetische Substitution eine sehr grosse Schlüsselmenge besitzt, ist sie dennoch überhaupt nicht sicher, da sie leicht durch Häufigkeitsanalyse geknackt werden kann. Gleichzeitig kann ein Kryptosystem mit einer kleinen Schlüsselmenge nie sicher sein, da es einfach ist, alle möglichen Schlüssel auszuprobieren. Eine grosse Schlüsselmenge ist also lediglich *notwendig*, aber *nicht hinreichend* für die Sicherheit eines Kryptosystems.

Jedes sichere Kryptosystem muss eine grosse Schlüsselmenge besitzen, aber nicht jedes Kryptosystem mit einer grossen Schlüsselmenge ist sicher!

Aufgabe 1.10

Entschlüsseln Sie den Text `ECRRCKZVRAZCRZK` mit dem Schlüssel aus Abbildung 1.8.

Aufgabe (Challenge) 1.11

Lösen Sie eine Knobelaufgabe in dem online-Kapitel *Substitution*.

Kapitel 2

Vigenère und One-Time-Pad: Zwei symmetrische Kryptosysteme

Zunächst möchten wir definieren, was symmetrische Kryptosysteme sind.

Definition 2.1 (Symmetrische Kryptosysteme)**:**
Ein Kryptosystem wird *symmetrisch* genannt, wenn die Information, die man zum Entschlüsseln benötigt, identisch mit der Information zum Verschlüsseln ist.

Beispiel 2.1 (symmetrische Kryptosysteme)**:**
Caesar, die allgemeine monoalphabetische Substitution sowie die Skytale sind Beispiele für symmetrische Kryptosysteme.

Caesar ist symmetrisch, da man zum Entschlüsseln die gleiche Information benötigt wie zum Verschlüsseln, nämlich die Anzahl der Verschiebungen. Wenn man beispielsweise weiss, dass der Text mit einer Verschiebung von 3 verschlüsselt worden ist, so kann man diesen Text mit einer Verschiebung von -3 wieder entschlüsseln.

In diesem Kapitel werden wir zwei weitere historisch bedeutende symmetrische Kryptosysteme kennen lernen: das Verfahren von Vigenère und das One-Time-Pad.

2.1 Das Kryptosystem *Vigenère*

Wie wir in Aufgabe 1.6 gesehen haben, ist es einfach, Texte, die mit Caesar verschlüsselt worden sind, anzugreifen, entweder mittels Buchstabenhäufigkeitsanalyse oder indem man einfach alle 26 möglichen Verschiebungen ausprobiert (Brute-Force-Angriff). Auch weitere monoalphabetische Substitutions-Verfahren wie das in Abbildung 1.8 gezeigte Verfahren, können durch eine Häufigkeitsanalyse und etwas Knobeln relativ einfach geknackt werden.

Idee 2.1 (Vigenère)**:**
Das zentrale Problem der allgemeinen monoalphabetischen Substitution (und somit auch von Caesar) ist, dass jeder Buchstabe im Klartext stets in denselben Buchstaben im Kryptotext umgewandelt wird (e.g. aus einem `E` im Klartext wird im Kryptotext immer ein `M`).

Die Grundidee von Vigenère ist es, dieses Problem zu umgehen, indem man als Schlüssel nicht nur einen einzigen Buchstaben, sondern ein ganzes Wort verwendet. Das Vorgehen wird in Definition 2.2 illustriert.

Definition 2.2 (Vigenère-Verfahren)**:**
Angenommen wir verwenden den Vigenère-Schlüssel (das Wort) `KEY`, um den Klartext

`INFORMATIKISTSOWASVONINTERESSANT`

zu verschlüsseln. Der Buchstabe `K` bewirkt eine Caesar-Verschiebung um Ord(`A`) = 10, der Buchstabe `E` eine Caesar-Verschiebung um Ord(`E`) = 4 und der Buchstabe `Y` schliesslich eine Caesar-Verschiebung um Ord(`Y`) = 24. Die Verschlüsselung erfolgt dabei wie folgt:

```
  Klartext: INF|ORM|ATI|KIS|TSO|WAS|VON|INT|ERE|SSA|NT
 Schlüssel: KEY|KEY|KEY|KEY|KEY|KEY|KEY|KEY|KEY|KEY|KE
Kryptotext: SRD|YVK|KXG|UMQ|DWM|GEQ|FSL|SRR|OVC|CWY|XX
```

Je nachdem, an welcher Position sich ein Buchstabe im Klartext befindet, wird dieser mit einem anderen Buchstaben des Schlüssels verschlüsselt. Dadurch wird die Häufigkeit eines Buchstabens im Klartext auf mehrere Buchstaben im Kryptotext verteilt, was die Häufigkeitsanalyse deutlich erschwert.

Sie sehen sofort, dass beispielsweise der Buchstabe `I` im Klartext, je nach seiner relativen Position zum Schlüssel, in genau einen der drei verschiedenen Buchstaben `S`, `G` oder `M` im Kryptotext umgewandelt wird. Die Situation für den Buchstaben `E` ist in Abbildung 2.1 dargestellt.

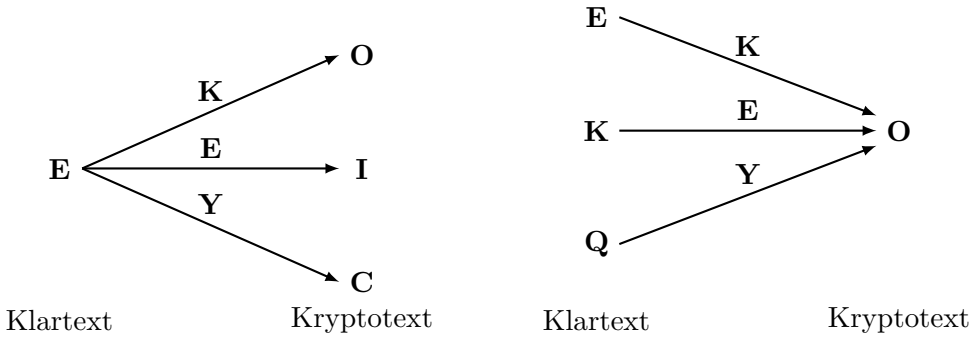


Abbildung 2.1: Verschlüsselungs-Möglichkeiten mit Vigenère, mit dem Schlüssel `KEY`

Bemerkung 2.1 (Caesar ist ein Spezialfall von Vigenère)**:**
Im Vergleich zum Verfahren von Vigenère, wird bei Caesar aus einem Buchstaben im Klartext immer derselbe Buchstabe im Kryptotext. Verwenden wir beispielsweise den Caesar-Schlüssel `K` (also eine Verschiebung von 10), so würde sich folgende Verschlüsselung ergeben:

```
  Klartext: I|N|F|O|R|M|A|T|I|K|I|S|T|S|O|W|A|S|V|O|N|I|N|T|E|R|E|S|S|A|N|T
 Schlüssel: K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K|K
Kryptotext: S|X|P|Y|B|W|K|D|S|U|S|C|D|C|Y|G|K|C|F|Y|X|S|X|D|O|B|O|C|C|K|X|D
```

Aus dem Buchstaben `I` im Klartext wird also stets der Buchstabe `S` im Kryptotext, unabhängig von seiner Position relativ zum Schlüssel.

Offensichtlich ist Caesar ein Spezialfall von Vigenère, bei dem der Schlüssel (das Wort) aus exakt einem einzigen Buchstaben besteht.

Aufgabe 2.1

Welche Eigenschaft muss ein Vigenère-Schlüssel haben, damit (zumindest theoretisch) aus einem Buchstaben im Klartext exakt 10 verschiedene Buchstaben im Kryptotext werden können? Geben Sie ein Beispiel für einen solchen Schlüssel an.

Das Verfahren von Vigenère galt während mehreren Jahrhunderten als sicher und wurde in zahlreichen vielen militärischen Anwendungen eingesetzt!

2.1.1 Vigenère-Tabelle und praktische Umsetzung

Wie bereits in Definition 2.2 angesprochen, definiert jeder Buchstabe eines Vigenère-Schlüssels eine bestimmte Caesar-Verschiebung. Es ist daher sinnvoll, eine Tabelle zu erstellen, welche jede der 26 möglichen Caesar-Verschiebungen auf einen Blick darstellt. Diese Tabelle wird als **Vigenère-Tabelle** bezeichnet und ist in Tabelle 2.1 gegeben. Jede der 26 Spalten der Vigenère-Tabelle entspricht einer möglichen Caesar-Verschiebung (Einstellung der Caesar-Drehscheibe), welche durch den entsprechenden Schlüsselbuchstaben definiert ist.

Klartextbuchstabe	Schlüsselbuchstabe																									
		(0) A	(1) B	(2) C	(3) D	(4) E	(5) F	(6) G	(7) H	(8) I	(9) J	(10) K	(11) L	(12) M	(13) N	(14) O	(15) P	(16) Q	(17) R	(18) S	(19) T	(20) U	(21) V	(22) W	(23) X	(24) Y	(25) Z
(0)	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
(1)	B	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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 2.1: Vigenère-Tabelle mit numerischer Ordnung

Verschlüsselung: Soll beispielsweise der Klartextbuchstabe `E` mit dem Schlüsselteil `K` verschlüsselt werden, so findet man in der Tabelle den entsprechenden Kryptotextbuchstaben `O`.

Entschlüsselung: Soll beispielsweise der Kryptotextbuchstabe `O` mit dem Schlüsselteil `K` entschlüsselt werden, so sucht man in der Tabelle nach dem Klartextbuchstaben, der mit `O` und `K` korrespondiert. Dies ist in diesem Fall der Buchstabe `E`.

Aufgabe 2.2

Verschlüsseln Sie folgenden Text von Hand, mit dem Schlüssel `YES` und mit der Methode von Vigenère:

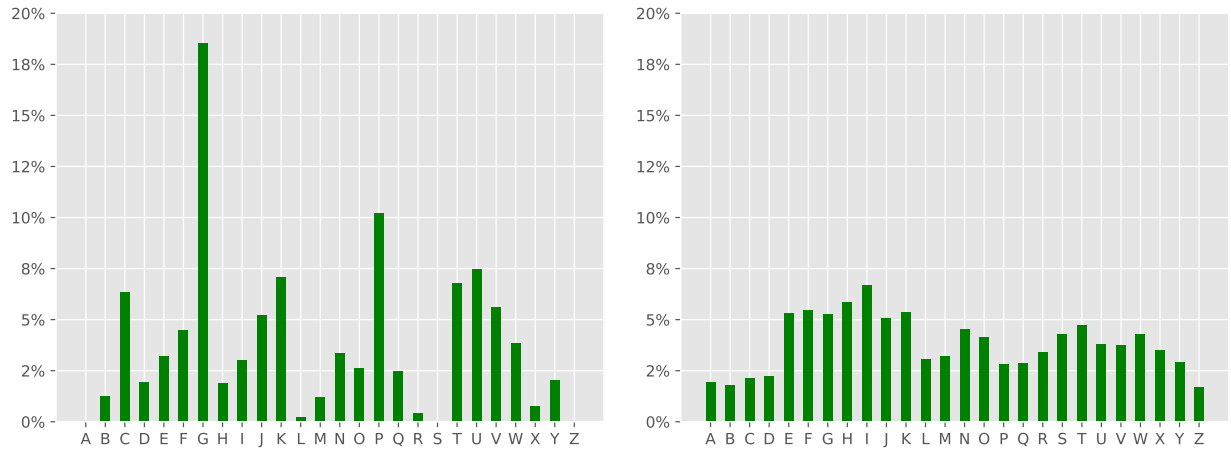
`NIEMANDKANNDASLESEN`

Aufgabe 2.3

Entschlüsseln Sie folgenden Text von Hand, wenn Sie wissen, dass er mit dem Schlüssel `TOP` und mit der Methode von Vigenère verschlüsselt worden ist:

`UFPOCVNHVXAPVVI`

Wir haben einen langen Klartext verwendet und diesen einmal mit Caesar (Schlüssel `C`, also Verschiebung 2)und einmal mit Vigenère (Schlüssel `ABCDEFG`) verschlüsselt und schliesslich die relativen Häufigkeit aller verschiedenen Buchstaben im Kryptotext in Abbildung 2.2 dargestellt. Die relative Häufigkeit eines Buchstabens im Kryptotext ist definiert als die Anzahl der Vorkommen dieses Buchstabens geteilt durch die Gesamtanzahl aller Buchstaben im Kryptotext



(a) Caesar (b) Vigenère

Abbildung 2.2: relative Häufigkeit der Buchstaben im Kryptotext eines langen Texts, einmal mit Caesar (Schlüssel: `C`) und einmal mit Vigenère (Schlüssel: `ABCDEFG`) verschlüsselt

Abbildung 2.2 zeigt, dass Vigenère zu einer insgesamt homogeneren Verteilung der relativen Buchstabenhäufigkeiten im Kryptotext führt. Dies kommt daher, dass bei Vigenère jeder Klartextbuchstaben auf *mehrere* Kryptotext-Buchstaben verteilt wird, währenddem bei Caesar jeder Klartextbuchstaben stets auf denselben Kryptotextbuchstaben abgebildet wird.

2.1.2 Kryptoanalyse von Vigenère

2.1.2.1 Kryptoanalyse von Vigenère bei bekannter Schlüssellänge

Wenn die Schlüssellänge eines mit Vigenère verschlüsselten Texts bekannt ist, kann man den Klartext relativ einfach herausfinden. Das Vorgehen ist exemplarisch in Beispiel 2.2 beschrieben.

Beispiel 2.2 (Häufigkeitsanalyse von Vigenère bei bekannter Schlüssellänge)**:**
Angenommen, wir wüssten, dass folgender Kryptotext durch die Verwendung eines Vigenère-Schlüssels der Länge 3 entstanden ist:

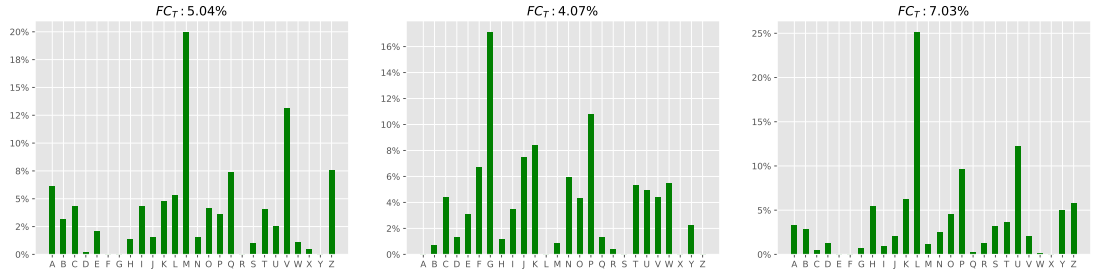
```
MKU MYB VFL ZDH ZGO MKA MTR MKA PCA UGP VGN IPG MUL MNL MKU OGU WOT MPN TGP KJK MPZ CGZ
AGU NTB MJS QPN AOV ZIL VFP MKJ POP BIH VBL UJL ZBL VIL VKL AUL QEO JKU INS MKU CPK NTL
CGT QEO UGP VGZ TGI MPZ QPK QGZ MTN MIL VFK QGM CGY AQS KJL AGL TGU OGZ KJH NHL VKZ BYP
MFP MOL QPL QEO JKU AQN TWL KMS QEO UGP VDL AVL ZUV OCU HKU LGT OGM CGO TGC WPY CJP OGT
```

LCZ MKU DGY AWU SGU LCZ AOL QPL SWU AVK ITB VVL ZNL QFL BKJ PMV MPU BGQ MVG BPP KJA HGP
KJU MPU QEO BGP VGU AVY QEO CPK JKU VKL MKU OTV MUZ MTL ZOH TGY OGD MUL VCS AKU LKL AGU
IWN MPI TKJ SGU EGU VFH ANP MDL

Alle grünen Buchstaben entstanden durch eine Verschiebung entsprechende dem ersten Buchstaben des Vigenère-Schlüssels, alle blauen Buchstaben durch eine Verschiebung entsprechend dem zweiten Buchstaben des Vigenère-Schlüssels und alle roten Buchstaben durch eine Verschiebung entsprechend dem dritten Buchstaben des Vigenère-Schlüssels.

Wenn wir die grünen, blauen und roten blauen Buchstaben jeweils zu einem eigenen Kryptotext zusammenfassen, erhalten wir drei verschiedene Kryptotexte, welche jeweils durch eine Caesar-Verschiebung entstanden. Damit können wir die auf jede der drei Gruppen (grün, blau, rot) die Häufigkeitsanalyse (genau analog zu Abschnitt 1.6) anwenden, um innerhalb der jeweiligen Gruppe die Verschiebung zu erraten, welche durch den entsprechenden Vigenère-Schlüsselbuchstaben definiert ist.

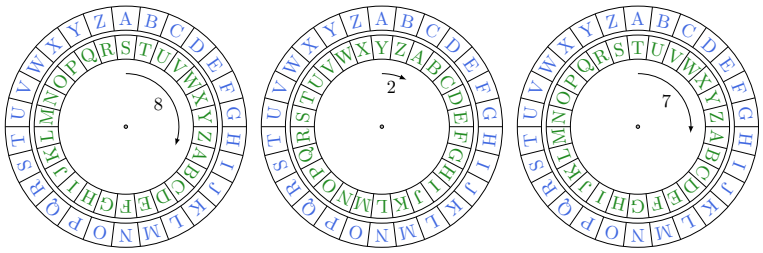
In Abbildung 2.3) sind die relativen Häufigkeiten der Buchstaben für jede der drei Gruppen dargestellt.



(a) grüne-Gruppe (b) blaue-Gruppe (c) rote-Gruppe

Abbildung 2.3: relative Buchstabenhäufigkeit in einem durch Vigenère verschlüsselten Text pro Gruppe

Dabei erkennen wir, dass die häufigsten Buchstaben pro Gruppe M, G, bzw. L sind. Da E der häufigste Buchstabe im Deutschen ist, können wir annehmen, dass die häufigsten Buchstaben M, G, bzw. L jeweils aus E im Klartext entstanden sind. Dies entspricht den folgenden drei Caesar-Verschiebungen: E→M entspricht einer Verschiebung von 8 (um I), E→G einer Verschiebung von 2 (um C) und E→L einer Verschiebung von 7 (um H).:



Der Vigenère-Schlüssel wird also vermutlich ICH lauten, da ord(I) = 8, ord(C) = 2 und ord(H) = 7.

Aufgabe 2.4

Kopieren Sie den folgenden Kryptotext und versuchen Sie, ihn mit dem Analysetool zu entziffern, wenn Sie wissen, dass die Schlüssellänge drei ist. Schauen Sie sich die Buchstabenhäufigkeiten für jede der 3 Gruppen an, indem Sie unter *Analysewerkzeug* die Häufigkeitsanalyse auswählen und *stride* (Schrittgrösse) 3. Unterhalb der Grafiken kann man zwischen jeder der drei Gruppen hin- und herwechseln. Probieren Sie den wahrscheinlichsten Schlüssel aus, indem Sie beim *Entschlüsselungswerkzeug* die Methode *Vigenère* auswählen und den Schlüssel eingeben.

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

Aufgabe 2.5 Vigenère knacken bei bekannter Schlüssellänge (zu dritt)

Finden Sie für folgenden Vigenère-Text den Klartext heraus, wenn Sie wissen, dass der Schlüssel Länge 3 hat:

```
WKJ LMU AKJ WZJ WQV WVV KBG ZBG JAV OMP FRG VMT WZM WVP LEK WMN WUG FBC JMK FMX WZN
SMU KTK UPG NMT KKJ DCG KAG DCP YNW WZW FAG JMH JMK ZMK LQU L
```

1. Finden Sie zuerst die häufigsten Buchstaben pro Gruppe heraus (Gruppe 3 ist bereits gemacht, s. unten). Seien Sie genau, ansonsten müssen Sie später wieder von vorne beginnen!

   Notizen

2. Finden Sie danach den Schlüssel heraus, indem Sie annehmen, dass der häufigste Buchstabe im Geheimtext den Buchstaben `E` im Klartext repräsentiert. Für Gruppe 3 ist die Lösung bereits vorgegeben.

	Häufigster Buchstabe	**Schlüssel**
Gruppe 1		
Gruppe 2		
Gruppe 3	`(E →) G`	`(A →) C` (=2 Verschiebungen)

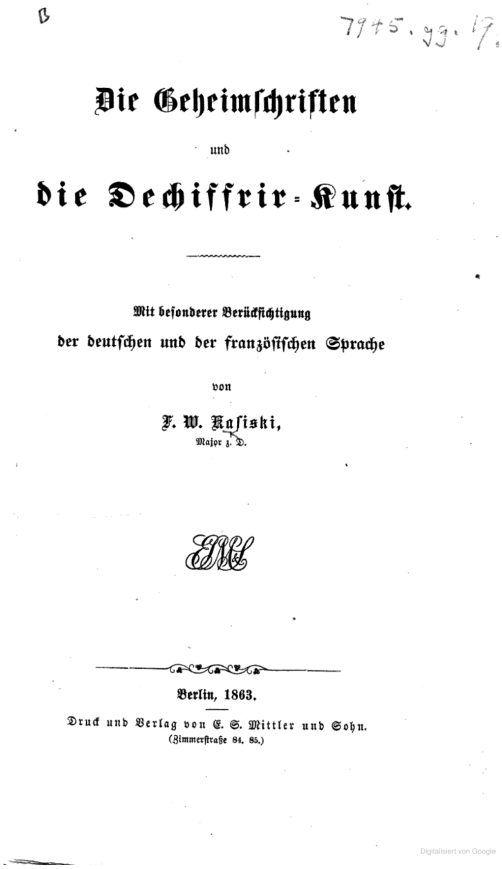
3. Entschlüsseln Sie nun den Geheimtext, indem Sie die Caesar-Drehscheiben verwenden (Tipp: Machen Sie jeweils eine Farbgruppe pro Mal).

```
--- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- ---
--- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- -
```

2.1.2.2 Bestimmung der Schlüssellänge mit dem Kasiski-Test

Wie Sie gesehen haben, kann man Vigenère *gruppenweise* mit denselben Methoden knacken, die wir benutzt haben, um Caesar zu knacken. Falls die Schlüssellänge unbekannt ist, können sowohl der Kasiski-Test wie auch die Friedmansche Charakteristik verwendet werden, um diese zu erraten. In diesem Unterabschnitt schauen wir uns zunächst den Kasiski-Test an.

Friedrich Kasiski war ein preussischer Infanteriemajor (1805 - 1881), welcher mit seinem Kasiski-Test massgeblich zum Knacken der Vigenère-Verschlüsselung beigetragen hat. Den Kasiski-Test veröffentlichte er 1863 in seinem Buch „Die Geheimschriften und die Dechiffrir-Kunst“ (siehe Abbildung 2.4).


B

7945. gg. 17.

Die Geheimſchriften

und

die Dechiffrir-Kunſt.

Mit beſonderer Berückſichtigung

der deutſchen und der franzöſiſchen Sprache

von

F. W. Kaſiski,

Major z. D.

Berlin, 1863.

Druck und Verlag von E. S. Mittler und Sohn.

(Zimmerſtraße 84, 85.)

Abbildung 2.4: Umschlag des Buches „Die Geheimschriften und die Dechiffrir-Kunst“ von Friedrich Kasiski (1863, Quelle)

Die Grundidee hinter dem Kasiski-Test ist: Wenn ein Wort oder ein Wortteil im Klartext mehrmals vorkommen, so wird dieser möglicherweise auch im Kryptotext mehrmals vorkommen. Wenn beispielsweise die Buchstaben `DIE` mehrmals mit dem Schlüssel `KEY` verschlüsselt werden, dann wird der Text `LIV` mehrmals im Geheimtext auftauchen. Wenn das Wort `DIE` also zweimal im Klartext vorkommt **und** auf denselben Schlüsselteil (`KEY`, `EYK` oder `YKE`) fällt, wird z.B. `LIV` auch zweimal im Kryptotext gleich verschlüsselt sein.

Wenn wir also im Kryptotext nach wiederholten Sequenzen suchen, können wir daraus die Schlüssellänge ableiten.

Beispiel 2.3:
In folgendem Beispiel ist der Klartext auf der ersten Zeile. Der Schlüssel `CODE` wird verwendet, um den Geheimtext (auf der dritten Zeile) zu erzeugen:

```
MEINKLEINERREIMSCHEINTKEINERZUSEIN

CODECODECODECODECODECODECODECODECO

OSLRMZHMPSUVGWPWEVHMPHNIKBHVBIVIKB
  2     7           19    24        32
```

Der Kasiski-Test erlaubt uns, Hinweise auf die Schlüssellänge zu erhalten, ohne den Schlüssel zu kennen:

- Die Sequenzen `HMP` und `IKB` erscheinen je zweimal im Geheimtext.
- Die Sequenz `HMP` befindet sich an den Positionen 7 und 19. Die Differenz zwischen diesen Positionen beträgt 12. Wenn beide `HMP` das gleiche Trigramm kodieren (in diesem Fall das Trigramm `EIN`), muss die Schlüssellänge ein Teiler von 12 sein.
- Die Sequenz `IKB` befindet sich an den Positionen 24 und 32. Die Differenz zwischen diesen Positionen beträgt 8. Wenn beide `IKB` das gleiche Trigramm kodieren, muss die Schlüssellänge ein Teiler von 8 sein.
- Die gemeinsamen Teiler von 12 und 8 sind 1, 2 und 4. Die Schlüssellänge muss einer dieser Teiler sein. Aus dieser Information alleine können wir die Schlüssellänge nicht eindeutig bestimmen, aber wir haben die Anzahl der Möglichkeiten bereits stark eingeschränkt. In diesem Fall ist die korrekte Schlüssellänge 4.

Aufgabe 2.6 Vigenère knacken bei bekannter Schlüssellänge (zu dritt)

Finden Sie den Klartext für folgende Nachricht heraus, wenn Sie wissen, dass der Text mit Vigenère verschlüsselt worden ist. Wenden Sie den Kasiski-Test an!

```
UEUIOOCEUDIWIOOWRRCLWVUQURRCLWVNDTHXETHERRCFKRTWVSFYOQRNJJTG
          10        20        30        40        50        60

RSVUAVIOOCEQEIHRUIYOHITQLNJZNJVSEVRJRUILNGUEUIOOCEUDIWIOOWHR
          70        80        90       100       110       120

VRWVAXWZXIOOCEQIOOWAWDEWVAXWUQUWRCLWVDLVNDVCKJTHETDXEYFMUFLO
          130       140       150       160       170       180

VRQZCKKSPVHUYOHIEQ
          190
```

Anleitung:

- Die Position an allen 10, 20, 30 etc. Buchstaben sind oben bereits markiert, ebenso wie Vorkommnisse des Trigramms IOO.
- Auf separatem Blatt:
  1. Notieren Sie sich die **Anfangspositionen** aller Trigramme IOO.
  2. Berechnen Sie die **Abstände** zwischen den Anfangspositionen. Es reicht, wenn Sie nur die Abstände aller Anfangspositionen von IOO zum ersten Trigramm IOO an Position 4 berechnen.
  3. Zerlegen Sie die Abstände zwischen den Trigrammen in **Primfaktoren**.
  4. Finden Sie den **grössten gemeinsamen Teiler** dieser Primfaktoren, um die Schlüssellänge zu erraten.
- Wenn Sie die Schlüssellänge haben, färben Sie den Text abwechslungsweise ein, wie in Aufgabe 2.5. Teilen Sie sich zu dritt auf, so dass jede Person eine Gruppe von Buchstaben entschlüsselt (gleich wie in Aufgabe 2.5).
- **Tipp**: Der letzte Teil des Schlüssels ist D. Der Schlüssel ergibt ein Wort. Entschlüsseln Sie den Text nun mit den Caesar-Drehscheiben! Entschlüsseln Sie zuerst nur die erste Zeile, um zu überprüfen, ob ihr Schlüssel stimmt und zu einem sinnvollen Text führt.

Aufgabe 2.7

Finden Sie die Schlüssellänge für folgenden Vigenère-Text heraus, indem Sie den Kasiski-Test anwenden:

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

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

Verwenden Sie dazu folgendes Online-Tool: https://cryptbreaker.marcwidmer.xyz/solve

1. Verwenden Sie das Analyse-Werkzeug *Kasiski-Analyse*, um die Abstände der sich wiederholenden Sequenzen der Länge 4 zu bestimmen.
   - Notieren Sie sich die Positionen und Abstände der sich wiederholenden Sequenzen der Länge 4.
   - Zerlegen Sie die Abstände in Primfaktoren.
   - Finden Sie den grössten gemeinsamen Teiler der Abstände, um die Schlüssellänge zu erraten.
2. Überprüfen Sie Ihre Vermutung, indem Sie im Analyse-Werkzeug die Häufigkeitsanalyse mit der Schrittweite (*stride*) gleich der vermuteten Schlüssellänge durchführen.
3. Entschlüsseln Sie den Text mit dem *Vigenère*-Entschlüsselungswerkzeug.

Aufgabe 2.8

1. Erklären Sie kurz: Dopplungen im Klartext (z.B. `EIN`) führen nicht unbedingt zu Dopplungen im Geheimtext.
2. Erklären Sie kurz: Dopplungen im Geheimtext müssen nicht in jedem Fall aus Dopplungen im Klartext stammen; sie können auch zufällig entstehen.

Aufgabe (Challenge) 2.9

Versuchen Sie, auf diesem Link eine weitere Challenge-Aufgabe zu lösen, indem Sie die Werkzeuge *Kasiski*, *Frequency* (Häufigkeit) und *Vigenère* verwenden:

2.1.2.3 Bestimmung der Schlüssellänge: Friedmansche Charakteristik

Eine weitere Möglichkeit, die Schlüssellänge zu erraten, besteht in der Verwendung der sogenannten Friedmanschen Charakteristik.

William Friedman (1891-1969) war ein russisch-amerikanischer Kryptologe und Pionier auf dem Gebiet der Kryptoanalyse (siehe Abbildung 2.5). Kurz vor dem Ausbruch des zweiten Weltkriegs gründete er den Signals Intelligence Service (SIS), eine Geheimabteilung des US-Militärs zur Entzifferung feindlicher Codes und Geheimschriften.

Abbildung 2.5: William Friedman (Quelle)

Die Friedmansche Charakteristik macht sich zunutze, dass Buchstaben im Klartext ungleich verteilt sind. Falls jeder Buchstabe gleich häufig vorkommen würde, wäre die erwartete Häufigkeit jedes Buchstabens genau 1/26. In keiner natürlichen Sprache besitzen alle Buchstaben dieselbe relative Häufigkeit. Die Häufigkeitsverteilung der Buchstaben in deutschen Texten haben wir bereits in Tabelle 1.1 gesehen. Die relative Häufigkeit des Buchstabens `E` in deutschen Texten ist beispielsweise ca. 17.4%. Die relative Häufigkeit eines Buchstabens $\square$ in einem Text T bezeichnen wir mit $h_{\square}(T)$.

Die Friedmansche Charakteristik berechnet, wie ungleich alle Buchstaben in einem Text verteilt sind, indem sie die quadrierte Differenz der relativen Häufigkeit jedes Buchstabens zu 1/26 berechnet. Diese quadrierten Abweichungen werden danach alle aufsummiert (siehe Gleichung (2.1)).

Bemerkung 2.2:
Das Quadrieren der Abweichungen (Differenzen) hat zwei Effekte:

- Quadrate von reellen Zahlen sind sicherlich nicht negativ.
- Grosse Abweichungen von 1/26 tragen aufgrund des Quadrierens überproportional zur Summe (zur Friedmanschen Charakteristik) bei.

$$FC(T) = \left(h_A(T) - \frac{1}{26}\right)^2 + \left(h_B(T) - \frac{1}{26}\right)^2 + \ldots + \left(h_Z(T) - \frac{1}{26}\right)^2 \tag{2.1}$$

$$= \sum_{\Delta \in \text{Alphabet}} \left(h_{\Delta}(T) - \frac{1}{26}\right)^2 \tag{2.2}$$

Eine stark ungleiche Verteilung von Buchstaben in einem Text T führt also zu einer hohen Friedmanschen Charakteristik $FC(T)$, währenddem gleichmässig verteilte Buchstaben im Text T zu einer tieferen $FC(T)$ führen. Deutschsprachige (Klar-)Texte haben durchschnittlich etwa einen Wert von 3.8% (0.038) (siehe Abbildung 2.6).

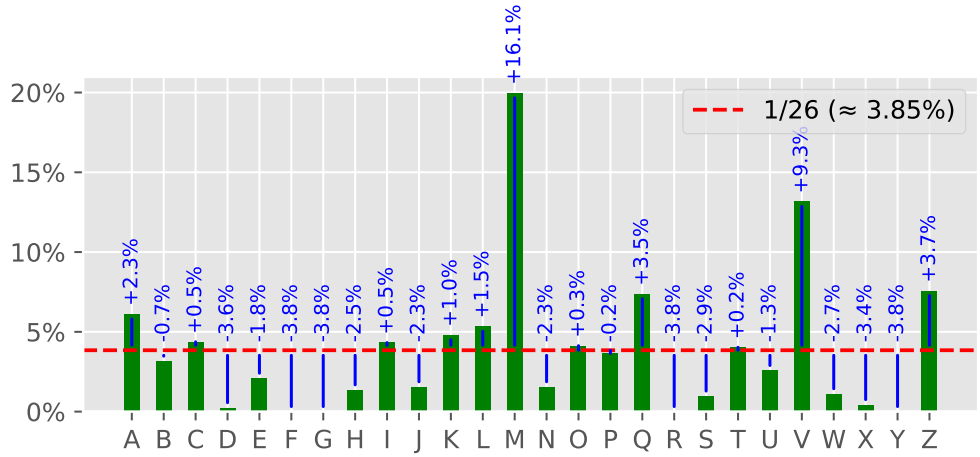
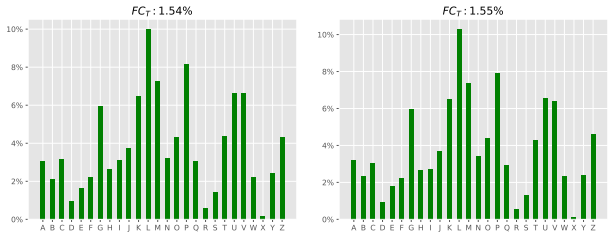


Abbildung 2.6: Buchstabenhäufigkeit in einem mit Caesar verschlüsselten Text, im Vergleich zur Gleichverteilung von Buchstaben

Je grösser die blauen Pfeile in Abbildung 2.6, desto höher die Friedmansche Charakteristik.

Wir können nun folgenden *Brute-Force*-Ansatz verwenden, um die Schlüssellänge mit der Friedmanschen Charakteristik zu bestimmen:

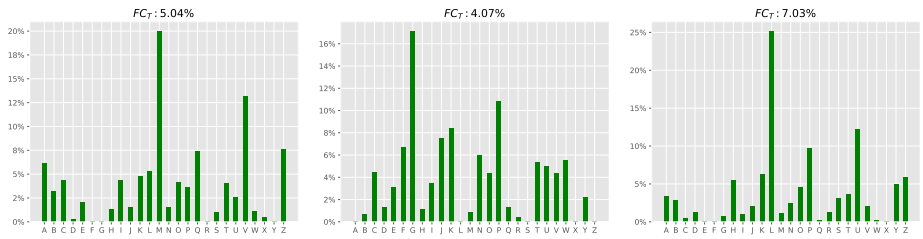
- Alle möglichen Schlüsselwortlängen von 1 bis zu einer beliebig gewählten Zahl n ausprobieren, wobei n praktisch nie über 10 gewählt wird.
- Buchstaben jeweils in Gruppen unterteilen:
  - **2 Gruppen**: MU ZK JL QP AW JU MH YI IL LC ZA UP MR LZ HL SV CM TZ BC UL GU PC IM PD QG TI PC QI LV GY MG UB UJ PN BM UZ MN AP GY HN PK JL OT HB WS IV PW PK IH B



(a) Gruppe 1 (b) Gruppe 2

Abbildung 2.7: Buchstaben-Häufigkeiten und FC_T für Schlüssellänge=2

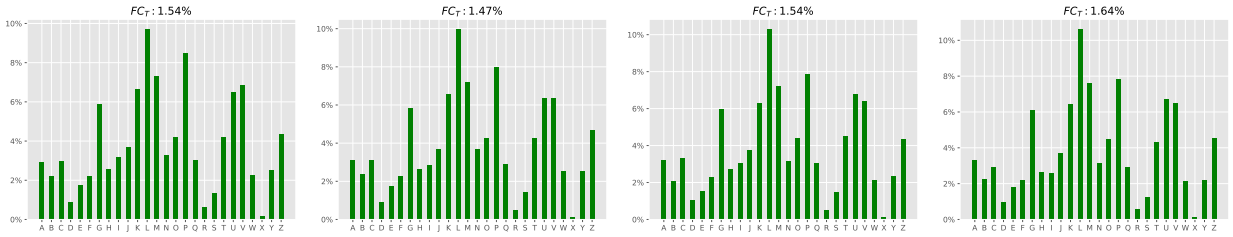
  - **3 Gruppen**: MUZ KJL QPA WJU MHY IIL LCZ AUP MRL ZHL SVC MTZ BCU LGU PCI MPD QGT IPC QIL VGY MGU BUJ PNB MUZ MNA PGY HNP KJL OTH BWS IVP WPK IHB



(a) Gruppe 1 (b) Gruppe 2 (c) Gruppe 3

Abbildung 2.8: Buchstaben-Häufigkeiten und FC_T für Schlüssellänge=3

  - **4 Gruppen**: MUZK JLQP AWJU MHYI ILLC ZAUP MRLZ HLSV CMTZ BCUL GUPC IMPD QGTI PCQI LVGY MGUB UJPN BMUZ MNAP GYHN PKJL OTHB WSIV PWPK IHB



(a) Gruppe 1 (b) Gruppe 2 (c) Gruppe 3 (d) Gruppe 4

Abbildung 2.9: Buchstaben-Häufigkeiten und FC_T für Schlüssellänge=4

  - etc, bis zu Schlüssellänge = n
- Für jede der Schlüssellängen: Durchschnittliche $FC(T)$ für alle Gruppen berechnen.
- Wenn die richtige Schlüssellänge (oder ein Vielfaches davon) gewählt wurde, sollte $FC(T)$ höher sein.

Die durchschnittliche Friedmansche Charakteristik für jede der getesteten Schlüssellängen ist gezeigt in Abbildung 2.10.

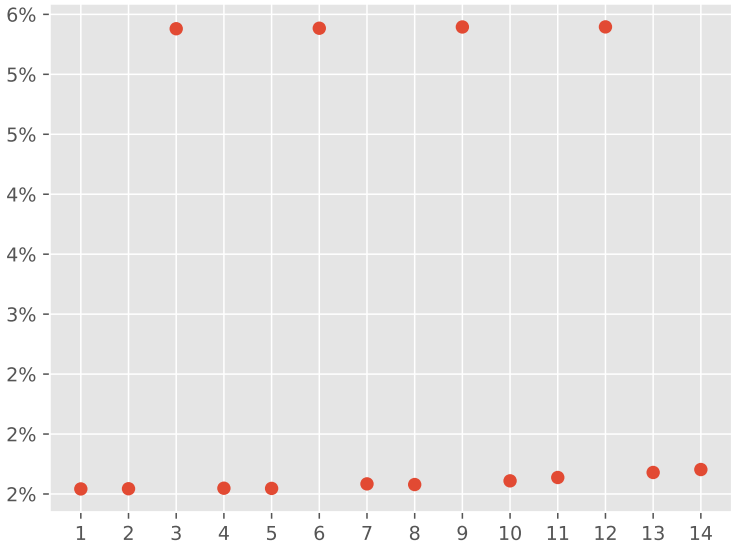


Abbildung 2.10: Durchschnittliche Friedmansche Charakteristik für jede Schlüssellänge

Aus Abbildung 2.10 lässt sich ablesen, dass die Schlüssellänge vermutlich 3 sein muss, da bei jedem Vielfachen der Schlüssellänge 3 die durchschnittliche Friedmansche Charakteristik höher ist als für die restlichen Schlüssellängen. Ab nun lässt sich gleich vorgehen wie in Unterabschnitt 2.1.2 beschrieben, um den Text zu entschlüsseln.

Aufgabe 2.10

Berechnen Sie die Friedmansche Charakteristik für folgende beide Texte von Hand:

P A P P E R L A P A P P

B A C K S T E I N

Wie interpretieren Sie die beiden Zahlen?

Aufgabe 2.11

Für welche Buchstabenverteilung sollte die Friedmansche Charakteristik höher sein: Abbildung 2.2, (a) oder (b)?

Aufgabe 2.12

Kopieren Sie den folgenden Kryptotext und versuchen Sie, ihn mit dem Analysetool zu entziffern, indem Sie zuerst das Tool *Friedman* und danach das Tool *Frequency* verwenden. Wie lautet der Schlüssel?

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

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

Aufgabe (Challenge) 2.13

Berechnen Sie die Friedmansche Charakteristik für folgenden Kryptotext:

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

Verwenden Sie dazu das Python-Skript auf Moodle, mit der Funktion `def calculate_fc(text)`. Was entnehmen Sie aus Ihrer Antwort? Wurde der Text mit Caesar oder mit Vigenère verschlüsselt?

Aufgabe (Challenge) 2.14 Ver- und Entschlüsselung mit Python (zu zweit)

Laden Sie zuerst die Vigenère-Python-Dateien von Moodle herunter. Erstellen Sie danach einen Text in deutscher Sprache mit mindestens 1000 Zeichen, beispielsweise mittels folgender Webseite: https://www.blindtextgenerator.de/. Diesen werden Sie nun mit Python verschlüsseln.

Teil 1: Verschlüsselung

- Verschlüsseln Sie Ihren Text, indem Sie die Funktion `def vigenere(text, key, encrypt=True)` verwenden.
- Senden Sie Ihren verschlüsselten Text an Ihre(n) Partner(in), nicht aber den Schlüssel.

Teil 2: Entschlüsselung

- Sie erhalten den Kryptotext und müssen nun zuerst den Schlüssel herausfinden. Bestimmen Sie diesen mithilfe der Friedmanschen Charakteristik, indem Sie die Funktion `def get_friedman_vals(text, maxkeylen)` verwenden.
- Nachdem Sie die Schlüssellänge bestimmt haben, finden Sie innerhalb jeder Gruppe dem häufigsten Buchstaben. Dies können Sie mit der Funktion `def show_letter_freq(text)` einfach umsetzen. Somit sollten Sie das Schlüsselwort herausfinden können.
- Entschlüsseln Sie nun den Kryptotext, indem Sie die Funktion `def vigenere(text, key, encrypt=False)` verwenden.

Aufgabe (Challenge) 2.15

Lösen Sie drei *beliebige Probleme* auf der Analyse-Webseite.

2.2 One-Time-Pad

Der Fortschritt in der Mathematik und das neu dazugekommene Wissen machten Vigenère zu einem unsicheren Kryptosystem.

Vigenère und dessen Kryptoanalyse haben wir bereits besprochen. Wir haben gesehen, dass eine

Kryptoanalyse vor allem dann leicht ist, wenn der verwendete Schlüssel zu kurz gewählt wird, denn die wesentliche Schwäche von Vigenère ist die Wiederholung der Muster im Kryptotext bei zu kurz gewähltem Schlüssel. Betrachten wir als Beispiel einen Kryptotext aus 1000 Buchstaben, der mit einem Schlüssel der Länge fünf verschlüsselt ist. Das bedeutet, dass jeder fünfte Buchstabe und somit insgesamt je 200 Buchstaben anhand der gleichen Zeile der Vigenère-Tabelle verschlüsselt sind. Das heisst, dass je 200 Buchstaben mit dem gleichen Schlüsselbuchstaben verschlüsselt sind. Durch eine Häufigkeitsanalyse von 200 Buchstaben kann ein Kryptoanalytiker bereits den entsprechenden Buchstaben des Schlüssels bestimmen. Was wäre aber, wenn der verwendete Schlüssel aus 50 Buchstaben bestehen würde? Dann muss eine Häufigkeitsanalyse von 50 Teilen zu je 20 Buchstaben gemacht werden. Es ist nicht garantiert, dass man aus nur 20 Buchstaben eine repräsentative Häufigkeitsverteilung erhält. Gehen wir noch einen Schritt weiter und wählen einen Schlüssel, der genau gleich lang ist wie der Klartext. Nun ist eine Häufigkeitsanalyse völlig unmöglich, da wir es mit 1000 Teilen zu je nur einem Buchstaben zu tun haben.

Die One-Time-Pad-Verschlüsselungsmethode (OTP, deutsch *Einmalschlüssel-Verfahren*) funktioniert im Prinzip identisch wie die Vigenère-Methode, mit folgenden drei Unterschieden:

1. Der Schlüssel besteht aus einer *zufälligen* Folge von Buchstaben
2. Der Schlüssel ist *genau gleich lang* wie der Klartext/Kryptotext
3. Der Schlüssel wird nur für genau eine Botschaft verwendet

Beispiel 2.4:
Folgendes Beispiel verwendet einen OTP-Schlüssel:

```
  Klartext: OERLIKON
 Schlüssel: IGBQPWXD
Kryptotext: WKSBXGLQ
```

Essentiell handelt es sich beim OTP um dasselbe Verschlüsselungsverfahren wie bei Vigenère, wobei der Schlüssel gleich lang wie die zu verschlüsselnde Nachricht sein muss. Diese Methode gilt als sicher, da die gruppenweise Häufigkeitsanalyse (z.B. mit der Friedmanschen Charakteristik) nicht funktioniert. Allerdings ist die OTP-Methode aufgrund der längeren Schlüssellänge mit höheren Übertragungskosten verbunden. Zudem darf jeder Schlüssel zur Sicherheit nur einmal verwendet werden, was für regelmässige Datenaustausch-Anwendungen wie E-Mail, Online-Banking etc. unpraktisch ist.

Vorgehen 2.1 (Kryptosystem OTP)**:**

Klartextalphabet: Alphabet der lateinischen Grossbuchstaben.
Kryptotextalphabet: Alphabet der lateinischen Grossbuchstaben.
Schlüsselmenge: alle denkbaren Texte, bestehend aus lateinischen Grossbuchstaben, welche dieselbe Länge haben wie der Klartext. Es ist wichtig, dass für jeden Klartext ein Schlüssel zufällig generiert wird.
Verschlüsselung: Gegeben ist ein zufällig gewählter Schlüssel s aus der Schlüsselmenge. Der gegebene Klartext wird nun (wie gewohnt) mit Hilfe der Vigenère-Tabelle mit dem Schlüssel s verschlüsselt. Der Schlüssel darf danach nicht mehr verwendet werden.
Entschlüsselung: Gegeben ist ein zufällig gewählter Schlüssel s aus der Schlüsselmenge. Der gegebene Kryptotext wird (wie gewohnt) durch Vigenère mit dem Schlüssel s entschlüsselt.

Warum erscheint uns das OTP als ein sicheres Kryptosystem? Die Intuition ist wie folgt. Weil der

Schlüssel zufällig gewählt wird und genauso lang ist wie der Klartext, wird jeder Buchstabe des Klartextes um zufällig viele Positionen im Alphabet verschoben. Damit kann man den Kryptotext als eine zufällige Folge von Buchstaben betrachten. Und aus einer zufälligen Folge von Buchstaben kann man keine Informationen herauslesen.

Alice und Bob haben sich in einem geheimen Treffen schon vor einigen Tagen auf den geheimen Schlüssel der Länge 5 für das OTP geeinigt. Alice verwendet nun den mit Bob vereinbarten Schlüssel, um eine geheime Nachricht (Kryptotext) an ihn zu senden. Der gesendete Kryptotext lautet `GVRCL`.

Eve hat den Nachrichtenaustausch belauscht und somit den Kryptotext in Erfahrung gebracht. Sie möchte nun den Klartext herausfinden um zu erfahren, was Alice und Bob unternehmen werden. Eve vermutet, dass der Kryptotext mit dem sicheren OTP verschlüsselt ist. Da der verwendete Schlüssel gleich lang ist wie der Klartext, ist eine Kryptoanalyse mit der Häufigkeitsanalyse unmöglich.

Aufgabe 2.16

(a) Wie viele mögliche Schlüssel der Länge 5 gibt es?
(b) Kann Eve den Kryptotext `GVRCL` entschlüsseln, falls sie (im schlimmsten Fall) alle Möglichkeiten durchprobiert?

Dennoch hat Eve das Gefühl, dass sie die geheime Nachricht erraten kann. Die Anzahl aller Klartexte, die aus fünf Buchstaben einen sinnvollen Text ergeben, wird vermutlich nicht so gross sein. Ausserdem weiss Eve, dass sich Alice und Bob verabreden wollen. Eve listet deshalb einige sinnvolle Texte zu je fünf Buchstaben auf. Für jeden dieser möglichen Klartexte bestimmt sie den Schlüssel (mit Hilfe der Vigenère-Tabelle), der den entsprechenden Text zu dem gegebenen Kryptotext `GVRCL` verschlüsseln würde.

möglicher Klartext	entsprechender Schlüssel
BADEN	FVOYY
ESSEN	CDZYY
LESEN	VRZYY
SPORT	OGDLS
VIDEO	LNOYX

Tabelle 2.2: Entsprechende Schlüssel bei geratenen möglichen Klartexten (BADEN, ESSEN, LESEN, SPORT, VIDEO) für abgehörten Kryptotext GVRCL.

Jeder dieser Texte kann also durch den angegebenen Schlüssel zum Kryptotext `GVRCL` verschlüsselt werden. Welcher Text entspricht nun der richtigen Nachricht? Alice und Bob haben ihren geheimen Schlüssel zufällig bestimmt, das heisst, jeder mögliche Schlüssel kann mit der gleichen Wahrscheinlichkeit ausgewählt werden. Eve hat daher keine Möglichkeit herauszufinden, welche dieser fünf möglichen Klartexte der geheimen Nachricht entspricht. Es ist auch möglich, dass der richtige Klartext nicht in der Liste steht. Somit hat Eve keine Chance irgendeinen Teil des Klartextes oder des Schlüssels zu erfahren.

Ein Hauptproblem aller symmetrischen Verschlüsselungsverfahren besteht jedoch darin, dass der Schlüssel erst einmal über einen *sicheren* Kanal ausgetauscht werden muss. Vor dem Internet erfolgte dies durch einen Postboten, heute ist dies allerdings nicht mehr praktikabel. Dies werden wir im nächsten Kapitel besprechen.

Aufgabe 2.17

Wie viele mögliche Schlüssel hat der OTP für eine Nachricht der Länge n?

2.2.1 Kryptoanalyse bei mehrfacher Verwendung des Schlüssels

Nun wollen wir wissen, weshalb ein Schlüssel beim OTP nur einmal verwendet werden darf. Dazu schauen wir uns einen erneuten Nachrichtenaustausch zwischen Alice und Bob an. Alice möchte Bob nämlich eine weitere geheime Nachricht schicken. Da die zwei jedoch zuvor keinen zweiten Schlüssel vereinbart haben, verwendet Alice den gleichen Schlüssel ein zweites Mal. Diesmal erhält Bob von Alice den folgenden Kryptotext: `ADRCM`.

Eve hat ihr Vorhaben, die beiden zu belauschen, noch nicht aufgegeben und versucht erneut die verschlüsselte Mitteilung zu lesen. Wenn Alice und Bob für die zweite Nachricht einen neuen zufälligen Schlüssel ausgemacht hätten, dann könnte Eve erneut nichts mit dem Kryptotext anfangen. Alice war jedoch nachlässig und verwendete den gleichen Schlüssel ein zweites Mal, um sich mit Bob zu verabreden. Eve ergänzt ihre Tabelle mit einer dritten Spalte. In dieser Spalte notiert sie den Klartext, der entsteht, wenn sie den zweiten Kryptotext mit dem entsprechenden Schlüssel aus der zweiten Spalte entschlüsselt.

möglicher Klartext	entsprechender Schlüssel	möglicher Klartext für die zweite Nachricht
BADEN	FVOYY	VIDEO
ESSEN	CDZYY	YASEO
LESEN	VRZYY	FMSEO
SPORT	OGDLS	FMSEO
VIDEO	LNOYX	PQDEP

Tabelle 2.3: Entschlüsselung eines weiteren abgehörten Kryptotextes (ADRCM) durch die vorher bestimmten denkbaren Schlüsselkandidaten. Der Schlüsselkandidat FVOYY erzeugt aus beiden abgehörten Kryptotexten einen sinnvollen Klartext.

Und siehe da, fast alle Texte in der dritten Spalte ergeben keinen Sinn, ausser dem Text in der ersten Zeile. Eve erkennt, dass mit dem Schlüssel FVOYY sowohl der erste wie auch der zweite Kryptotext zu einem sinnvollen Text entschlüsselt werden können. Durch den Vergleich der Entschlüsselungen des ersten und des zweiten Kryptotextes bei gleichem Schlüssel konnte Eve die tatsächlichen Klartexte und den Schlüssel herausfinden.

2.2.2 Bin-OTP

Das Kryptosystem Bin-OTP funktioniert fast gleich wie das OTP, nur dass wir nicht mit dem lateinischen Alphabet der Grossbuchstaben arbeiten wollen, sondern lediglich mit dem binären Alphabet $\{0, 1\}$. Aus der grossen Vigenère-Tabelle in Tabelle 2.1 wird im binären Alphabet die übersichtliche (binäre) Vigenère-Tabelle:

Klartextbuchstabe \ Schlüsselbuchstabe	0	1
0	0	1
1	1	0

Abbildung 2.11: Vigenère-Tabelle für das binäre Alphabet.

Der Tabelle entnehmen wir, dass der Klartextbuchstabe 0 durch den Schlüssel 0 zum Kryptotextbuchstaben 0 wird. Man verwendet für die Verschlüsselung mit der binären Vigenère-Tabelle eine besondere Schreibweise. Für die Verschlüsselung des Klartextbuchstaben 0 durch den Schlüssel 0 schreiben wir

$$0 \oplus 0 = 0.$$

Wird 0 durch 1 verschlüsselt erhalten wir den Kryptotextbuchstaben 1 (siehe Tabelle) und schreiben

$$0 \oplus 1 = 1.$$

Bitte beachten Sie, dass auch

$$1 \oplus 0 = 1$$

sowie

$$1 \oplus 1 = 0$$

gilt. Die Verschlüsselung mit dem binären OTP erfolgt nun, indem Bit für Bit die Operation $\oplus$ (gemäss binärer Vigenère-Tabelle) durchgeführt wird. Analog haben wir mit den lateinischen Buchstaben auch die Verschlüsselung Buchstabe für Buchstabe mithilfe der Vigenère-Tabelle durchgeführt.

Beispiel 2.5:
Folgendes Beispiel illustriert, wie die Verschlüsselung mit dem Bin-OTP funktioniert:

- Der Klartext ist gegeben durch 101 und der Schlüssel durch 111. Dann ist der Kryptotext gegeben durch $101 \oplus 111 = 010$:

$$\begin{array}{rccc} & 1 & 0 & 1 \\ \oplus & 1 & 1 & 1 \\ \hline & 0 & 1 & 0 \end{array}$$

- Der Klartext ist gegeben durch 011101 und der Schlüssel durch 110001. Dann ist der Kryptotext gegeben durch

$$011101 \oplus 110001 = 101100.$$

Aufgabe 2.18

Berechnen Sie den Kryptotext zu dem gegebenen Klartext

$$110010100$$

und zum Schlüssel

$$101110001.$$

Aufgabe 2.19

(a) Berechnen Sie sowohl

$$100110 \oplus 001011$$

als auch

$$001011 \oplus 100110.$$

Was stellen Sie fest?

(b) Seien a und b zwei beliebige Bits. Begründen Sie, warum stets die Gleichheit

$$a \oplus b = b \oplus a$$

gilt. Wie heisst diese Eigenschaft?

Aufgabe 2.20

Sei a eine beliebige binäre Folge (denken Sie sich z.B. $a = 1100101$).

(a) Was macht die Verschlüsselung $a \oplus a$ von a mit sich selbst?

(b) Mit 0 bezeichnen wir im Folgenden eine Folge aus lauter Nullen derselben Länge wie a. Was macht die Operation $a \oplus 0$?

Es lässt sich beweisen, dass die Operation $\oplus$ auch *assoziativ* ist. Die Klammerung der Terme spielt also keine Rolle. Für beliebige binäre Folgen a, b und c derselben Länge gilt also

$$(a \oplus b) \oplus c = a \oplus (b \oplus c).$$

Dies gilt auch für mehr als drei Operanden.

Aufgabe 2.21

Es sei t ein gegebener (binärer) Klartext. Alice wählt zufällig einen binären Schlüssel s_A derselben Länge wie t und berechnet

$$k_A := t \oplus s_A.$$

Was erhält Alice, wenn sie nun

$$k_A \oplus s_A$$

berechnet, also ihren Schlüssel erneut anwendet?

Kapitel 3

Schlüsseltausch-Verfahren

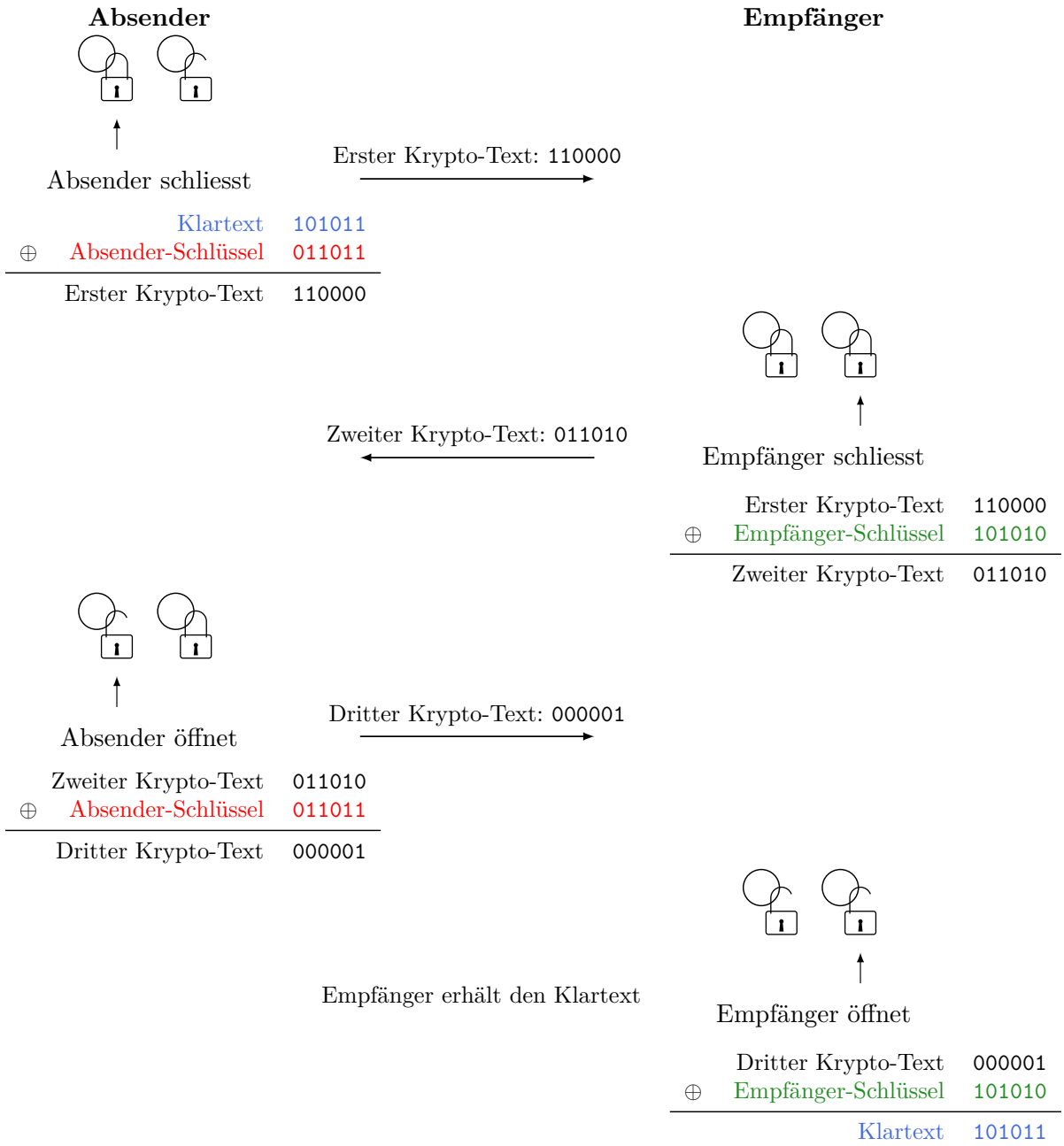


Abbildung 3.1: Schlüsseltausch mit öffentlichen Schlüsseln

3.1 Drei-Wege-Schlüsseltausch

Vorgehen 3.1 (Kommunikationsprotokoll Three-Pass Protocol)**:**
Das Kommunikationsprotokoll Three-Pass Protocol (auch Schlüsseltausch mit drei Durchgängen genannt) ermöglicht es Alice, einen geheimen Schlüssel t an Bob zu senden, ohne dass sie zuvor einen gemeinsamen geheimen Schlüssel vereinbart haben. Dazu verwenden sowohl Alice als auch Bob jeweils einen eigenen zufälligen Schlüssel (s_A bzw. s_B).

Ausgangssituation: Alice besitzt einen zufälligen binären Schlüssel s_A der Länge n. Bob besitzt ebenfalls einen zufälligen binären Schlüssel derselben Länge n.

Ziel: Alice hat zuvor einen geheimen binären Schlüssel t der Länge n gewählt. Diesen Schlüssel (das ist hier der Klartext) möchte sie über einen unsicheren Kanal an Bob senden, ohne dass Unbefugte den Schlüssel erfahren.

1. **A**lice verschlüsselt den zu verschickenden Schlüssel t (Klartext) mit ihrem Schlüssel s_A:

   $$k_A := t \oplus s_A$$

   und sendet den entstandenen Kryptotext k_A an Bob.
2. **B**ob verschlüsselt die empfangene Nachricht k_A nun auch mit seinem Schlüssel s_B:

   $$k_{AB} := k_A \oplus s_B$$

   und sendet den Kryptotext k_{AB} zurück an Alice.
3. Alice entschlüsselt den Kryptotext k_{AB} mit ihrem Schlüssel s_A:

   $$k_B = k_{AB} \oplus s_A$$

   und sendet k_B an Bob.
4. Schliesslich entschlüsselt Bob den Kryptotext k_B mit seinem Schlüssel s_B:

   $$t = k_B \oplus s_B$$

   und erhält dadurch den Klartext t, welchen Alice ihm mitteilen möchte.

Warum funktioniert das? Der Kern der Geschichte liegt darin, dass eine zweite Anwendung eines Schlüssels die erste Anwendung desselben Schlüssels löscht (rückgängig macht) und zwar, auch wenn zwischen diesen zwei Anwendungen andere Schlüssel angewendet worden sind. Betrachten Sie die folgende Berechnung

$$\begin{aligned} &t \oplus s_A \oplus s_B \oplus s_A \oplus s_B = \\ &t \oplus (s_A \oplus s_A) \oplus (s_B \oplus s_B) = \\ &t \oplus 0 \oplus 0 = t. \end{aligned}$$

Aufgabe 3.1

Spielen Sie den Schlüsseltausch mit einer weiteren Person aus der Klasse durch.

Sicherheit des Drei-Wege-Schlüsseltauschs

Ist das Drei-Wege-Kommunikationsprotokoll sicher? Bietet es dieselbe Sicherheitsgarantie wie die Verwendung einer Truhe mit zwei Schlössern?

Wenn ein Kryptoanalyst nur einzelne Kryptotexte des Protokolls erhält und das Verfahren nicht kennt, wirkt die Kommunikation als eine Folge von Zufallsbits und in diesem Sinne ist unsere Implementierung dieses Verfahrens sicher. Wir müssen aber damit rechnen, dass der Angreifer das Kommunikationsprotokoll kennt (oder errät) und die zwei zufällig generierten Schlüssel das Einzige sind, was ihm unbekannt ist.

Wenn der Angreifer (Eve) alle drei Kryptotexte (k_A, k_{AB}, k_B) abfangen kann, kann er durch die folgenden Berechnungen den Klartext t herausfinden:

$$
\begin{aligned}
& k_A \oplus k_{AB} \oplus k_B = \\
& (t \oplus s_A) \oplus (k_A \oplus s_B) \oplus (k_{AB} \oplus s_A) = \\
& (t \oplus s_A) \oplus (k_A \oplus s_B) \oplus ((k_A \oplus s_B) \oplus s_A) = \\
& t \oplus (s_A \oplus s_A) \oplus (s_B \oplus s_B) \oplus (k_A \oplus k_A) = \\
& t \oplus 0 \oplus 0 \oplus 0 = \\
& t.
\end{aligned}
$$

3.2 Diffie-Hellman-Merkle-Schlüsseltausch

Vorgehen 3.2 (Protokoll Diffie-Hellman-Merkle (DHM))**:**
Das Kommunikationsprotokoll DHM ermöglicht es Alice und Bob, gemeinsam über einen öffentlichen Kanal einen geheimen Schlüssel zu vereinbaren, ohne dass sie zuvor einen gemeinsamen geheimen Schlüssel ausgemacht haben. Im Gegensatz zum Drei-Wege-Schlüsseltausch basiert das DHM-Protokoll auf der Schwierigkeit, das diskrete Logarithmusproblem zu lösen, ein mathematisches Problem, zu dem es (bisher) keinen effizienten Lösungsalgorithmus gibt.

Ausgangssituation: Alice und Bob haben sich zuvor öffentlich auf eine grosse Primzahl p und eine positive natürliche Zahl g geeinigt. Dabei ist g kleiner als p.

Ziel: Alice und Bob möchten gemeinsam mit einer öffentlichen Kommunikation einen Schlüssel s_{AB} vereinbaren. Diesen Schlüssel darf keine Drittperson in Erfahrung bringen.

1. Alice wählt zufällig eine positive ganze Zahl a mit $a < p$ und hält diese geheim. Dann berechnet sie mit dieser geheimen Zahl:
$$x := g^a \mod p$$
und sendet x an Bob.
2. Bob wählt zufällig eine positive ganze Zahl b mit $b < p$ und hält diese geheim. Dann berechnet er die Zahl
$$y := g^b \mod p$$
und sendet y an Alice.
3. Alice erhält y von Bob und berechnet mit ihrer geheimen Zahl a die Zahl
$$s_{AB} := y^a \mod p.$$
4. Bob berechnet mit dem erhaltenen x und seiner geheimen Zahl b die Zahl
$$s_{BA} := x^b \mod p.$$

Mithilfe der Rechengesetze der Modulo-Operation kann bewiesen werden, dass tatsächlich
$$s_{AB} = s_{BA}$$
gilt und somit Alice und Bob dieselbe Zahl berechnet haben. Diese Zahl s_{AB} ist der gemeinsame Schlüssel.

Aufgabe 3.2

Führen Sie das DHM-Protokoll mit einer weiteren Person aus der Klasse durch. Verwenden Sie
$$p := 13 \quad \text{und} \quad g := 2$$
(Sie können auch eigene Werte wählen) als öffentlich bekannte Schlüssel.

Aufgabe 3.3

Versuchen Sie das Kommunikationsprotokoll DHM zu knacken, indem Sie für die gegebenen Werte p, g, x und y jeweils die geheimen Zahlen a und b berechnen und daraus dann den vereinbarten Schlüssel s_{AB}.

(a) $g = 3, p = 5, x = 4, y = 2$
(b) $g = 2, p = 13, x = 6, y = 11$

Sicherheit des DHM-Protokolls

Das DHM-Protokoll ist sicher, weil es (bisher) keinen effizienten Algorithmus gibt, um das diskrete Logarithmusproblem zu lösen. Ein Kryptoanalyst (Eve) kann zwar die öffentlichen Werte p, g, x und y in Erfahrung bringen, aber um daraus den gemeinsamen Schlüssel s_{AB} zu berechnen, müsste sie entweder die geheime Zahl a von Alice oder die geheime Zahl b von Bob bestimmen. Dies entspricht dem Lösen des diskreten Logarithmusproblems, was (bisher) als schwierig gilt.

Allerdings ist das DHM-Protokoll nicht gegen einen Man-in-the-Middle-Angriff geschützt. Ein Angreifer (Eve) könnte sich zwischen Alice und Bob schalten und so tun, als ob sie Alice wäre, wenn sie mit Bob kommuniziert, und umgekehrt. Dadurch könnte Eve sowohl mit Alice als auch mit Bob jeweils einen eigenen gemeinsamen Schlüssel vereinbaren und so die Kommunikation zwischen den beiden belauschen. Diese Schwäche kann durch die Verwendung von digitalen Signaturen behoben werden, welche die Authentizität der Kommunikationspartner sicherstellen. Ein Beispiel eines solchen Signaturverfahrens ist das Rivest–Shamir–Adleman (RSA)-Kryptosystem (siehe Abschnitt 4.1).

Kapitel 4

Asymmetrische Kryptosysteme

In den bisher angeschauten Verschlüsselungsverfahren haben wir festgestellt, dass derselbe Schlüssel zur Ver- und Entschlüsselung verwendet wird. Daher spricht man bei diesen Verfahren von *symmetrischen* Verschlüsselungsmethoden. Zudem haben wir gesehen, dass diese entweder unsicher (Caesar, Vigenère) sind, wenn der Schlüssel einfach geknackt werden kann, oder unpraktikabel (OTP), wenn der Schlüssel zuerst übertragen werden muss. Diffie & Hellman kamen daher 1975 auf die Idee, *asymmetrische* Verschlüsselungsverfahren zu erschaffen, welche nach einem anderen Prinzip funktionieren. Im Gegensatz zu symmetrischen Verfahren kann man bei asymmetrischen Verfahren *nicht* von der verschlüsselten Nachricht auf den Schlüssel schliessen, da unterschiedliche Schlüssel zum Ver- und Entschlüsseln verwendet werden.

Die Grundidee hinter asymmetrischen Verschlüsselungsmethoden ist folgende:

Alice (👩‍💻) und Bob (👨‍💻) möchten auf verschlüsselte Weise Nachrichten austauschen, die den Anforderungen an sichere Kryptosysteme genügen (siehe Abschnitt 1.1). Bei der asymmetrischen Verschlüsselung generieren sowohl Alice wie Bob jeweils ein Schlüsselpaar, einen sogenannten **öffentlichen Schlüssel** (🔑), der von allen Personen gesehen und verwendet werden kann, sowie einen **privaten Schlüssel** (🔒), der nur im Besitz von Alice bzw. Bob ist. Wenn Alice eine Nachricht an Bob senden will, verwendet sie Bobs *öffentlichen* Schlüssel, um die Nachricht zu verschlüsseln. Die Nachricht kann jedoch mit dem öffentlichen Schlüssel nicht entschlüsselt werden, es handelt sich hier sozusagen um eine *Einweg*-Funktion. Stattdessen muss Bob seinen *privaten* Schlüssel zur Entschlüsselung verwenden, also den Schlüssel, auf den *nur* Bob Zugriff hat (siehe Abbildung 4.1). Dies funktioniert in den meisten Fällen auch in die andere Richtung: eine Nachricht, die mit Bobs privatem Schlüssel verschlüsselt worden ist, kann nur mit Bobs öffentlichem Schlüssel entschlüsselt werden. Die Schlüssel sind mathematisch so konstruiert, dass es beinahe unmöglich ist, vom öffentlichen Schlüssel auf den privaten Schlüssel zu schliessen.

Durch den Aufbau asymmetrischer Verschlüsselungsverfahren entfällt die Problematik der Übermittlung des Schlüssels: jede Person generiert ihr eigenes Schlüsselpaar und stellt einen öffentlichen Schlüssel zur Verfügung. Ein Nachteil hierbei ist, dass die Verschlüsselung häufig mathematisch und bezüglich Rechenleistung anspruchsvoller ist, was insbesondere problematisch sein kann bei längeren Nachrichten oder wenn die Antwortzeit minimal sein soll.

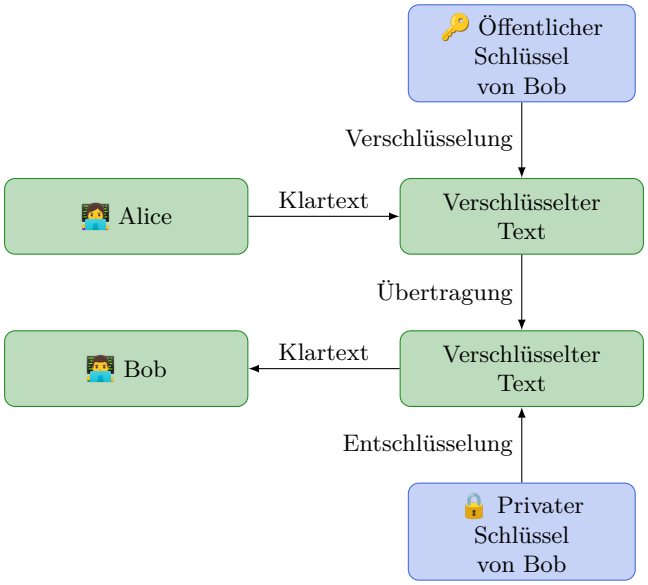


Abbildung 4.1: Prinzip der Public-Key-Verschlüsselung

4.1 RSA-Verfahren

Das Rivest–Shamir–Adleman (RSA)-Verfahren ist ein asymmetrisches Kryptosystem, das sowohl für die Verschlüsselung als auch für digitale Signaturen verwendet werden kann. Es basiert auf der Schwierigkeit, grosse Zahlen in ihre Primfaktoren zu zerlegen. Im Folgenden werden die Grundlagen des Verfahrens und ein einfaches Beispiel vorgestellt.

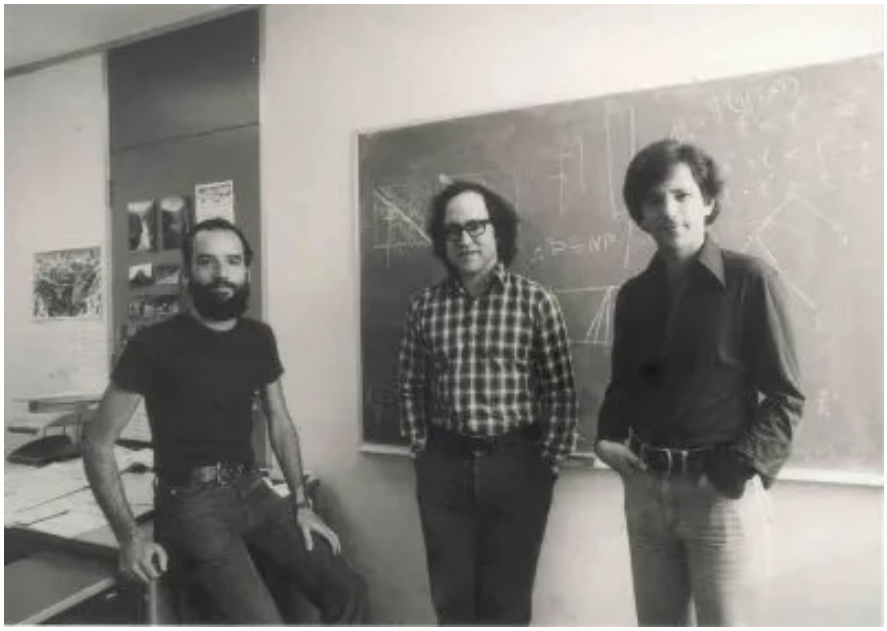


Abbildung 4.2: Ron Rivest, Adi Shamir und Leonard Adleman, die Erfinder des RSA-Verfahrens

Vorgehen 4.1 (RSA-Verschlüsselungsverfahren)**:**
Das RSA-Verfahren besteht aus folgenden Schritten:

1. **Schlüsselerzeugung:**

- Wählen Sie zwei (möglichst grosse) Primzahlen p und q.
- Berechnen Sie das RSA-Modul $n = p \cdot q$.
- Berechnen Sie die Eulersche Funktion $\varphi(n) = (p-1)(q-1)$.
- Wählen Sie den *Verschlüsselungsexponenten* e, so dass dieser teilerfremd zu $\varphi(n)$ und kleiner als $\varphi(n)$ ist. Dies bedeutet, dass der Grösster Gemeinsamer Teiler (GGT) von e und $\varphi(n)$ 1 ist ($\text{ggT}(e, \varphi(n)) = 1$).
- Berechnen Sie den *Entschlüsselungsexponenten* d, so dass $(e \cdot d) \mod \varphi(n) = 1$ (privater Schlüssel). Dies bedeutet, dass, wenn man d mit e multipliziert und dieses Produkt Modulo $\varphi(n)$ rechnet, man die Zahl 1 erhält.
- Die Zahlen p, q und $\varphi(n)$ werden nun nicht mehr benötigt und können gelöscht werden.

2. **Verschlüsselung:**
   - Der Absender verschlüsselt eine **Klartext-Nachricht m** (als Zahl) mit dem **öffentlichen Schlüssel** $(\mathbf{e}, \mathbf{n})$:
   $$c = \mathbf{m}^e \mod n$$
   - Das Ergebnis c ist der Kryptotext.
3. **Entschlüsselung:**
   - Der Empfänger entschlüsselt die **verschlüsselte Nachricht c** mit dem **privaten Schlüssel** $(\mathbf{d}, \mathbf{n})$:
   $$\mathbf{m} = c^d \mod n$$
   - Das Ergebnis **m** ist die ursprüngliche Nachricht.

Beispiel 4.1:
Um RSA besser zu verstehen, rechnen wir ein einfaches Beispiel mit kleinen Zahlen durch:

1. Wir wählen zwei (für diese Übung kleine) Primzahlen aus, $p = 3$ und $q = 11$. Daraus folgt:
$$\begin{aligned} n &= p \cdot q \\ &= 3 \cdot 11 \\ &= 33 \end{aligned}$$
$$\begin{aligned} \varphi(n) &= (p-1)(q-1) \\ &= 2 \cdot 10 \\ &= 20 \end{aligned}$$
2. Wir wählen $e = 3$, da $\text{ggT}(3, 20) = 1$.
3. Wir berechnen d, so dass $(e \cdot d) \mod \varphi(n) = 1$ ergibt:
$$(d \cdot 3) \mod 20 = 1 \quad \rightarrow \quad d = 7.$$
4. Der öffentliche Schlüssel ist $(e, n) = (3, 33)$, der private Schlüssel $(d, n) = (7, 33)$.

Verschlüsselung: Die Nachricht sei der Klartext `Code`, welches wir darstellen durch die Position der Buchstaben im Alphabet $m = 3, 15, 4, 5$. Berechne für jeden Buchstaben (hier

nur für `C`, also 3, gezeigt):

$$\begin{aligned} c &= m^e \mod n \\ &= 3^3 \mod 33 \\ &= 27 \mod 33 \\ &= 27. \end{aligned}$$

Der erste Buchstabe des Kryptotext wird also verschlüsselt als $c = 27$.

Entschlüsselung:

$$\begin{aligned} m &= c^d \mod n \\ &= 27^7 \mod 33 \\ &= 3 \end{aligned}$$

Daraus ergibt sich $m = 3$, also die ursprüngliche Nachricht.

Aufgabe 4.1

Alice möchte eine Nachricht an Bob mit RSA verschlüsseln. Bob wählt die Hilfs-Primzahlen $p = 5$ und $q = 7$. Generieren Sie den öffentlichen Schlüssel (e, n) und den privaten Schlüssel (d, n) von Bob, indem Sie folgende Schritte ausführen:

1. Berechnen Sie n und $\varphi(n)$.
2. Sie wählen e und d aus.

Verschlüsseln Sie nun die Nachricht $m = 9$ mit dem öffentlichen Schlüssel (e, n).

Entschlüsseln Sie danach die verschlüsselte Nachricht c wieder mit dem privaten Schlüssel (d, n).

Aufgabe 4.2

Ist die Wahl von p und q im obigen Beispiel sinnvoll? Begründen Sie Ihre Antwort.

Aufgabe (Challenge) 4.3

Erstellen Sie nun zu zweit jeweils ein Schlüsselpaar mit dem RSA-Verfahren. Verwenden Sie dazu Primzahlen p und q mit jeweils mindestens 2 Ziffern. Tauschen Sie danach Ihre öffentlichen Schlüssel aus und verschlüsseln Sie eine Nachricht (eine Zahl) an Ihren Partner. Entschlüsseln Sie danach die Nachricht wieder.

Eine Liste der ersten 1000 Primzahlen finden Sie hier: `https://en.wikipedia.org/wiki/List_of_prime_numbers`.

Aufgabe (Challenge) 4.4

Verwenden Sie Ihre RSA-Schlüssel aus 4.3, um eine echte Nachricht als Zahl auszutauschen (ein Wort). Um ein Wort in Zahlen umzuwandeln (Buchstabe für Buchstabe) können Sie folgendes Python-Skript verwenden:

```
def text_to_numbers(text):
    numbers = []
    for char in text.upper():
        if char.isalpha():  # Nur Buchstaben berücksichtigen
            numbers.append(ord(char) - ord('A') + 1)  # A=1, B=2, ..., Z=26
    return numbers

print(text_to_numbers("ABC"))  # Ausgabe: [1, 2, 3]
```

Aufgabe (Challenge) 4.5

Wählen Sie zwei Primzahlen p und q mit jeweils mindestens 3 Ziffern. Generieren Sie den öffentlichen und privaten Schlüssel. Verschlüsseln Sie eine Nachricht Ihrer Wahl und entschlüsseln Sie diese wieder. Verwenden Sie Python, um die Berechnungen durchzuführen.

Die Zahl d kann in Python folgendermassen berechnet werden:

Eine Liste der ersten 1000 Primzahlen finden Sie hier: https://en.wikipedia.org/wiki/List_of_prime_numbers

```
d = pow(e, -1, phi_n)
```

4.1.1 Digitale Signaturen mit RSA

Neben der Verschlüsselung von Nachrichten kann das RSA-Verfahren auch zur Erstellung digitaler Signaturen verwendet werden. Digitale Signaturen dienen dazu, die Authentizität und Integrität einer Nachricht zu gewährleisten. Hierbei wird die Nachricht mit dem privaten Schlüssel des Absenders signiert, sodass der Empfänger die Signatur mit dem öffentlichen Schlüssel des Absenders überprüfen kann.

Vorgehen 4.2 (Digitale Signaturen mit RSA)**:**
Die Erstellung und Überprüfung digitaler Signaturen mit dem RSA-Verfahren erfolgt in folgenden Schritten:

1. **Signaturerstellung:**
   - Der Absender erstellt eine **Nachricht m**.
   - Er berechnet den **Hashwert** $H(m)$ der Nachricht m mithilfe einer kryptographischen Hashfunktion (z.B. SHA-256).
   - Der Absender signiert den Hashwert mit seinem **privaten Schlüssel** $(\mathbf{d}, \mathbf{n})$:
   $$s = H(m)^d \mod n$$
   - Das Ergebnis s ist die digitale Signatur.
2. **Signaturüberprüfung:**
   - Der Empfänger erhält die Nachricht m und die Signatur s.
   - Er berechnet den Hashwert $H(m)$ der empfangenen Nachricht m.

- Der Empfänger überprüft die Signatur mit dem **öffentlichen Schlüssel** $(\mathbf{e}, \mathbf{n})$ des Absenders:
$$H'(m) = s^e \mod n$$
- Wenn $H'(m) = H(m)$, ist die Signatur gültig, andernfalls ist sie ungültig.

Beispiel 4.2:
Angenommen, Alice möchte eine Nachricht $m = 42$ signieren. Sie verwendet ihren privaten Schlüssel $(d, n) = (9677, 12317)$ und den öffentlichen Schlüssel $(e, n) = (5, 12317)$.

Signaturerstellung:

$$\begin{aligned} s &= H(m)^d \mod n \\ &= 42^{9677} \mod 12317 \\ &= 161 \end{aligned}$$

Die digitale Signatur ist also $s = 161$.

Signaturüberprüfung:

$$\begin{aligned} H'(m) &= s^e \mod n \\ &= 161^5 \mod 12317 \\ &= 42 \end{aligned}$$

Da $H'(m) = H(m)$, ist die Signatur gültig.

Aufgabe 4.6

Alice möchte die Nachricht $m = 15$ signieren. Ihr privater Schlüssel ist $(d, n) = (7, 33)$ und ihr öffentlicher Schlüssel ist $(e, n) = (3, 33)$.

Erstellen Sie die digitale Signatur s für die Nachricht m.

Überprüfen Sie danach die Signatur mit dem öffentlichen Schlüssel.

Anhang A

Python-Übungen zu Kryptologie

A.1 Allgemeine Zeichenketten-Aufgaben

Zeichenketten können verkettet, also aneinandergehängt werden mit dem Befehl `"Text1" + "Text2" + "Text3"` usw. Falls Sie eine Zeichenkette mehrfach drucken wollen, können Sie diese mit einer Zahl multiplizieren, die dann die Anzahl Wiederholungen der Zeichenkette bestimmt. So ist der Ausdruck `"a" * 3` beispielsweise gleichbedeutend mit einer Zeichenkette `"aaa"`.

Im Nachfolgenden schauen wir uns einige Übungen an, mit denen wir die einzelnen Zeichen aus Zeichenketten herauslesen können.

Aufgabe A.1

Führen Sie das nachfolgende Programm aus und erklären Sie, was das Programm tut.

```
text = "EASY"
for buchstabe in text:
  print(buchstabe)
```

Aufgabe A.2

Führen Sie das nachfolgende Programm aus und erklären Sie, was das Programm tut.

```
Klartext = "Schweiz"
print(Klartext[0])
print(Klartext[1])
print(Klartext[2])
print(Klartext[3])
print(Klartext[4])
print(Klartext[5])
print(Klartext[6])
```

Aufgabe A.3

Führen Sie das nachfolgende Programm aus und erklären Sie, was das Programm tut.

```
Klartext = "Schweiz"
for i in range(len(Klartext)):
  print(Klartext[i])
```

Der Befehl `for i in range(len(Klartext))` erstellt eine Variable `i` innerhalb der `for`-Schleife, welche jedes Zeichen von 0 bis zur Länge von `Klartext` minus 1 geht. Weshalb minus 1? Das erste Zeichen von `Klartext` wird in Python mit `Klartext[0]` ausgelesen, das letzte mit `Klartext[len(Klartext)-1]`, da wir bei 0 zu zählen beginnen und nicht bei 1. Mit dem Ausdruck `Klartext[i]` wird also das `i`-te Zeichen der Zeichenkette `Klartext` ausgelesen, wobei `i` von 0 bis zu (Länge des Klartexts minus 1) geht.

Der Befehl `for i in range(len(Klartext))` kann auch geschrieben werden als Befehl `for i in range(0, len(Klartext), 1)`, wobei dies meint:

- `i` beginnt bei 0
- `i` geht bis zu `len(Klartext)-1`
- `i` vergrössert sich in 1er-Schritten

Dieser Befehl könnte auch verwendet werden, um bei einer beliebigen Zahl zu starten (nicht notwendigerweise 0), und um `i` in Schritten grösser als 1 zu vergrössern. Die allgemeine Syntax des Befehls lässt sich also wie folgt zusammenfassen: `for i in range(start, ende, schrittgroesse)`.

Aufgabe (Challenge) A.4

Eine Person verrät uns lediglich die Vorwahl ihrer 10-stelligen Mobiltelefonnummer. Zudem verrät sie Ihnen auch, dass ihre Telefonnummer gerade ist (also auf 2, 4, 6, 8 oder 0 endet). Damit gibt es nur noch 5 Millionen Kombinationen, die es (im schlimmsten Fall) auszuprobieren gilt. Schreiben Sie ein Python-Programm, welches die 200 kleinsten, geraden Nummern auflistet. Die erste Nummer sollte 0790000000 sein, die letzte 0790000198. Das Programm soll die Nummern als Zeichenkette (eine Nummer pro Zeile) ausgeben.

Tipps:

- Mit `str(num)` wird aus der Zahl `num` eine Zeichenkette. Beispielsweise gibt uns `str(15)` die Zeichenkette `"15"`.
- Erinnern Sie sich, was die Operation `+` in dem Ausdruck `"In" + "form" + "atik"` macht?

A.2 Verschlüsselung von Texten in Python

Während des Zweiten Weltkriegs arbeitete der brillante Mathematiker Alan Turing in Bletchley Park im Vereinten Königreich und war mit der entscheidenden Aufgabe betraut, den Enigma-Code zu knacken, den die Deutschen zur Verschlüsselung ihrer Nachrichten verwendeten. Um diesen komplexen Code zu entschlüsseln, musste Turing sein tiefes Verständnis von Sprache und Mustern nutzen. In diesem Kapitel folgen wir in Turings Fussstapfen und entziffern einige Geheimnachrichten!

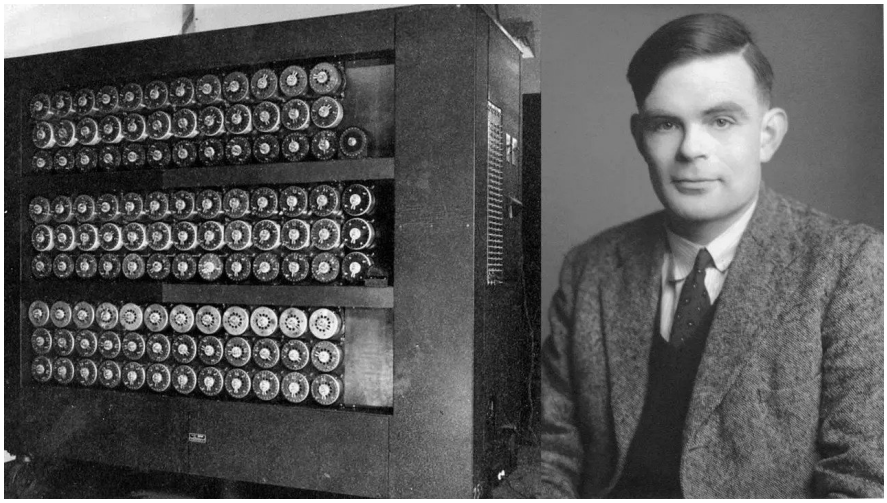


Abbildung A.1: Alan Turing

Im Nachfolgenden schauen wir uns einige Python-Befehle an, die dazu dienen, mit Zeichenketten (= engl. *strings*) zu arbeiten. Dies werden wir insbesondere benötigen, um eigene Python-Programme zu schreiben, mit denen wir Texte verschlüsseln und entschlüsseln können. Genauer gesagt bezeichnen wir Texte in Python als Zeichenketten. Zeichenketten werden in Python innerhalb von einfachen oder doppelten Anführungszeichen geschrieben, also entweder `'...'` oder `"..."`. Innerhalb der Anführungszeichen können beliebige Zeichen stehen, beispielsweise Buchstaben, Leerzeichen, Spezialzeichen oder Zahlen.

Tabelle A.2 enthält eine Übersicht einiger nützlicher Befehle, die Sie in diesem Kapitel verwenden werden.

Python	Beschreibung	Beispiel
`len(s)`	Gibt die Länge des Textes `s` zurück.	`n = len("hallo") # 5`

`s[index]`	Greift auf das Zeichen an der Index-Position `index` zu. Bei negativen Indizes zählt man von rechts.	`s = "hallo"`
		`s[0]  # "h"`
		`s[1]  # "a"`
		`s[-1] # "o"`

`s[start:end]`	Extrahiert den Teiltext vom Index `start` bis und ohne `end`	`text = "hallo"` `text[1:4] # "all"`

`ord(c)`	Gibt die Position des Zeichens `c` in der Unicode-Tabelle zurück	`ord('A') # 65`
		`ord('B') # 66`
		`ord('Z') # 90`

`chr(n)`	Gibt das Zeichen an der `n`-ten Position der Unicode-Tabelle zurück	`chr(65) # "A"`
		`chr(66) # "B"`
		`chr(67) # "C"`

`text1.count(text2)`	Zählt, wie oft der Text `text2` im Text `text1` vorkommt	`text = "Das Haus ist gross und das Dach ist grün."` `n = text.count("ist") # 2`
`text1.find(text2)`	Gibt den niedrigsten Index des Teiltexts `text2` zurück, falls dieser vorhanden ist, ansonsten `-1`	`text = "Das Haus ist gross und das Dach ist grün."` `text.find("ist") # 9`
`text.replace(old, new)`	Ersetzt alle Vorkommen des Teil-Texts `old` durch `new`.	`text = "hallo"` `text = text.replace("a", "e") # "hello"`

`text.split(sep)`	Zerlegt den Text an jedem `sep` und gibt eine Liste der Teiltexte zurück.	`text = "a,b,c"`
		`liste_texte = text.split(",")`
		`# ["a", "b", "c"]`

`sep.join(liste)`	Verbindet die Elemente von `liste` zu einem Text, getrennt durch den Text `sep`.	`txt = ":".join(["a", "b", "c"])` `# "a:b:c"`
`str(n)`	Zahl `n` in einen Text (engl. *string*) umwandeln	`zahl = 10` `zahl_als_text = str(zahl) # "10"`
`int(s)`	Text `s` in eine ganze Zahl (engl. *integer*) umwandeln	`zahl_als_text = "10"` `zahl = int(zahl_als_text) # 10`

Tabelle A.2: Übersicht von Zeichenketten-Befehlen

Aufgabe A.5

Schreiben Sie ein Programm, um jeden Buchstaben „e“ oder „E“ des folgenden Texts durch den Buchstaben „a“ oder „A“ zu ersetzen:

```
my_text = "Eines Tages entschied der Elefant, einen edlen Teppich zu weben."
```

Aufgabe A.6

Schreiben Sie ein Programm, um zu zählen, wie häufig der Buchstabe „e“ oder „E“ im gesamten folgenden Text vorkommt:

```
my_text = "Eines Tages entschied der Elefant, einen edlen Teppich zu weben."
```

Aufgabe (Challenge) A.7

Was könnte der Nutzen davon sein, dass es zwei Möglichkeiten gibt und nicht nur eine, Zeichenketten zu schreiben (`'...'` oder `"..."`)?

Mit der **Länge** von Zeichenketten ist die Anzahl der Zeichen zwischen den Anführungszeichen gemeint: Die Zeichenkette `"Hello World"` hat beispielsweise eine Länge von 11 Zeichen. Die Länge einer Zeichenkette kann mit dem Ausdruck `len(Klartext)` bestimmt werden.

Aufgabe A.8

Bestimmen Sie die Länge Ihres vollen Namens mithilfe des Befehls `len()` in Python.

```
n = "Vorname Nachname"
print(len(n)) # 16
```

Die Lösung für Aufgabe 1.4 könnte in Python wie folgt implementiert werden:

```
def zweiertausch(klartext):
    geheimtext = ""  # leerer String
    b = 0
    while b < (len(klartext) - 1):
        geheimtext += klartext[b + 1] + klartext[b]
        b += 2

    if len(klartext) % 2 != 0:
        # Klartexte ungerader Länge
        geheimtext += klartext[len(klartext) - 1]

    print(geheimtext)

# Verwendung:
# zweiertausch("KANTONSSCHULE")
```

Aufgabe A.9

Schreiben Sie eine Python-Funktion `def dreiertausch(klartext)`, welche den „Dreiertausch“ aus der Einführungsaufgabe 2 implementiert.

Aufgabe A.10

Schreiben Sie eine Python-Funktion `def umkehren(klartext)`, welche alle Zeichen eines Klartexts in umgekehrter Reihenfolge ausgibt.

Aufgabe A.11

Der Schlüssel für einen Geheimtext ist in Blöcken organisiert:

```
geheime_zahl_als_text = "2_10_38"
```

Trennen Sie die Blöcke von `geheime_zahl_als_text` in eine Liste auf und addieren Sie die Zahlen der Liste zusammen.

Als Resultat sollten Sie die Zahl 50 erhalten.

Aufgabe A.12

Verbinden Sie die Wörter in der Liste `liste = ["Der", "Code", "wurde", "geknackt"]` mit Leerzeichen zu einem vollständigen Satz.

A.3 Caesar-Verschlüsselung in Python

Aufgabe A.13

Entwickeln Sie eine Funktion, die zwei Parameter entgegennimmt: den Klartext (nur Grossbuchstaben!) und den Schlüssel (0-25). Als erstes soll jeder Buchstaben des Klartexts auf einer neuen Zeile ausgegeben werden.

Beispiel: Falls der Text `HALLO` eingegeben wird, soll folgendes ausgegeben werden:

```
H
A
L
L
O
```

Aufgabe A.14

Passen Sie das Programm aus Aufgabe 1.13 so an, dass statt den Buchstaben die Position in der Unicode-Tabelle ausgegeben wird. Verwenden Sie dafür die Funktion `ord()`.

Beispiel: Falls der Text `HALLO` eingegeben wird, soll folgendes ausgegeben werden:

```
72
65
76
76
79
```

Aufgabe A.15

Passen Sie das Programm aus Aufgabe 1.14 so an, dass Sie zu den Unicode-Positionen auch noch die Verschiebung hinzurechnen.

Beispiel: Falls der Text `HALLO` eingegeben wird und die Verschiebung 2, soll folgendes ausgegeben werden:

```
74
67
78
78
81
```

Aufgabe A.16

Passen Sie das Programm aus Aufgabe 1.15 so an, dass Sie statt den verschobenen Unicode-Positionen die Buchstaben ausgeben. Verwenden Sie dafür die Funktion `chr()`.

Beispiel: Falls der Text `HALLO` eingegeben wird und die Verschiebung 2, soll folgendes ausgegeben werden:

```
J
C
N
N
Q
```

Aufgabe A.17

Wenn man den Klartext `ZORRO` mit dem Schlüssel 14 verschlüsselt, erhält man mit dem Programm aus Aufgabe Aufgabe 1.16 den Geheimtext `h]``]`. Eigentlich sollte man aber den Geheimtext `NCFFC` erhalten. Lösen Sie das Problem!

Tipp: Der grösste gültige Unicode-Wert für Grossbuchstaben ist 90 für den Buchstaben „`Z`“. Wenn man einen Wert bekommt, der 91 oder grösser ist, muss man ihn verkleinern!

Aufgabe A.18

Passen Sie das Programm aus Aufgabe 1.17 so an, dass die Geheimtextbuchstaben nicht untereinander, sondern auf derselben Zeile in die Ausgabe geschrieben werden.

Tipp: Mit dem Operator `+` lassen sich in Python Texte miteinander verbinden.

```
text = ""
text += "Hello"
text += " Bob"
print(text) # Hello Bob
```

Die verschlüsselte Zeichenkette soll per `return`-Befehl zurückgegeben werden.

Aufgabe A.19

Entwickeln Sie ein Programm, das über einen Parameter den Geheimtext und den Schlüssel entgegennimmt und dann mit Hilfe der Caesar-Chiffre den Klartext wiederherstellt. Testen Sie es anschliessend, indem Sie eine verschlüsselte Nachricht von Ihrer Sitznachbarin oder Ihrem Sitznachbar entschlüsseln!

A.4 Vigenère-Verschlüsselung in Python

Aufgabe A.20

Entwickeln Sie eine Funktion `def vigenere(text, key)`, die über die zwei Parameter `text` und `key` einen Klartext sowie einen Schlüssel entgegennimmt. Das Programm soll den Klartext mit der Vigenère-Chiffre und mit dem Schlüssel verschlüsseln.

Aufgabe A.21

Entwickeln Sie eine Funktion `def vigenere_ent(text, key)`, die über die zwei Parameter `text` und `key` einen Geheimtext sowie einen Schlüssel entgegennimmt. Das Programm soll den Geheimtext mit der Vigenère-Chiffre und mit dem Schlüssel entschlüsseln.

Aufgabe (Challenge) A.22

Sie wollen all ihre Passwörter auf einer lokalen Textdatei abspeichern. Dies ist jedoch nicht sicher, denn falls jemand ihren Computer knackt, kann die Person alle Passwörter einsehen. Sie kommen auf folgende Idee: Statt die Passwörter aufzuschreiben, speichern Sie eine mit Vigenère verschlüsselte Variante davon. So müssen Sie sich lediglich den Vigenère-Schlüssel im Kopf merken, nicht aber ihre Passwörter. Verwenden Sie Ihr Programm aus Aufgabe 1.20, um ein Programm zu schreiben, das sie zuerst mit `input` nach einem Schlüssel und einem verschlüsselten Passwort fragt. Das Programm gibt Ihnen danach ihr Passwort im Klartext zurück.

Aufgabe A.23 Häufigkeitsanalyse und Caesar

Eine Nachricht wurde abgefangen: `msg = "AZDIYDHRZNOZI"`.

- Die Nachricht wurde mit der Caesar-Chiffre verschlüsselt. Finden Sie zunächst einmal den häufigsten Buchstaben in der verschlüsselten Nachricht. **Tipp**: „A“ und „Z“ haben die Positionen 65 und 90 im Unicode. Um in einer Schleife alle Zahlen von `x` by `y` durchzugehen, können Sie Folgendes schreiben: `for num in range(x, y+1):`.
- Bestimmen Sie den verwendeten Schlüssel, indem Sie die Funktion `ord()` zweimal verwenden.
- Ermitteln Sie den Klartext mithilfe Ihres Programms aus Aufgabe 1.18. **Tipp**: Das häufigste Zeichen in einem deutschen Text ist in der Regel „E“.
- Ersetzen Sie am Schluss im Klartext das Wort „WESTEN“ durch „OSTEN“.

Aufgabe A.24

Gegeben sei die durchschnittliche Buchstabenhäufigkeit für alle Buchstaben des deutschen Alphabets. Diese lässt sich berechnen, indem man die Häufigkeiten für sehr lange deutsche Texte aufsummiert.

```
german_letter_frequencies = [6.51, 1.89, 3.06, 5.08, 17.40, 1.66, 3.01,
    4.76, 7.55, 0.27, 1.21, 3.44, 2.53, 9.78, 2.51, 0.79, 0.02, 7.00, 7.27,
    6.15, 4.35, 0.67, 1.89, 0.03, 0.04, 1.13]
```

Berechnen Sie mithilfe des folgenden Python-Programms die Friedmansche Charakteristik für diese Häufigkeiten.

```
import matplotlib.pyplot as plt
import matplotlib.ticker as mtick
import numpy as np
from helpers import count_letters


def calculate_fc(text):
    # Determine the Friedman Characteristic for a given text
    summe = 0
    freq = count_letters(text)
    for letter_freq in freq:
        summe += (letter_freq - (1 / 26)) ** 2
    return summe


def friedman_slice(text, keylength):
    # Based on a text encrypted with Friedman and a given keylength,
    determine the average Friedman characteristic for all subgroups of the
    text.
    i = 0
    fc_avg = 0
    for i in range(keylength):
        text_slice = text[i::keylength]
        fc = calculate_fc(text_slice)
        fc_avg += fc
        i += 1

    fc_avg /= keylength

    return fc_avg


def get_friedman_vals(text, maxkeylen):
    """
    For a Text text, get the average Friedman Characteristics for key
    lengths up to maxkeylen
    """
    n = range(1, maxkeylen)
```

```
    fc = []
    for i in n:
        fc.append(friedman_slice(text, i))
    return fc


def draw_friedman(i, fc, turtle=False):
    """
    Draw the friedman Characteristics for various possible key lengths
    """
    if turtle:
        xshift = 150
        setPos(-xshift + 50, 150)
        label("friedman'sche Charakteristik:")
        setPos(-xshift, 0)
        pd()
        fd(200)
        bk(200)
        rt(90)
        fd(400)
        bk(400)

        for i in n:
            setPos(i * 40 - xshift, fc[i - 1] * 1000)
            dot(10)
            setPos(i * 40 - xshift, fc[i - 1] * 1000 + 40)
            label(i)
    else:
        fig, ax = plt.subplots()
        ax.plot(range(1, i), fc, "o")
        plt.xticks(np.arange(1, i, 1.0))
        ax.yaxis.set_major_formatter(mtick.PercentFormatter(decimals=0, xmax
   =1))
        return fig, ax


if __name__ == "__main__":
    print(calculate_fc("PAPPERLAPAPP"))
    print(calculate_fc("BACKSTEIN"))
```

Anhang B

Lernziele Kryptologie

- ☐ Ich weiss wie die folgenden Kryptosysteme funktionieren (Verschlüsselung und Entschlüsselung bei gegebenem Schlüssel):
  - ☐ Skytale
  - ☐ Caesar
  - ☐ Vigenère
  - ☐ One-Time-Pad
  - ☐ RSA
- ☐ Ich kenne die Grundbegriffe: Klartext, Kryptotext, Verschlüsselung (Chiffrierung), Entschlüsselung (Dechiffrierung), Schlüssel, Kryptografie / Kryptologie, Kryptosystem.
- ☐ Ich kenne die grundlegenden Sicherheitsziele: Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit (Nichtabstreitbarkeit) und kann sie kurz erläutern.
- ☐ Ich kann das Kerckhoffsche Prinzip erklären.
- ☐ Ich kann einen Caesar-Kryptotext durch Ausprobieren aller 25 Verschiebungen knacken (Brute-Force) und erkenne den richtigen Klartext.
- ☐ Ich kann einen Kryptotext, der durch die Vigenère-Verschlüsselung entstanden ist, mit Hilfe des Tools auf folgender Webseite entschlüsseln: Link zum Cryptbreaker
- ☐ Ich kann die Idee der Häufigkeitsanalyse erklären.
- ☐ Ich kann eine gruppenweise Häufigkeitsanalyse durchführen, um Vigenère bei bekannter Schlüssellänge zu knacken.
- ☐ Ich kann erläutern, weshalb eine kurze Schlüssellänge Vigenère schwächt (Wiederholungsmuster, Aufteilung in Gruppen) und warum lange bzw. OTP-lange Schlüssel nicht angreifbar durch Häufigkeitsanalyse sind.
- ☐ Ich kann den Unterschied zwischen monoalphabetischer und polyalphabetischer Substitution erklären.
- ☐ Ich kann einen monoalphabetisch substituierten Text mittels Häufigkeitsanalyse und schrittweisem Erraten entschlüsseln.
- ☐ Ich kann die Friedmansche Charakteristik für einen kurzen Text von Hand berechnen.
- ☐ Ich kann mit der Friedmanschen Charakteristik die Länge eines Vigenère-Schlüssels bestimmen.
- ☐ Ich kann erklären, was mit der Friedmanschen Charakteristik berechnet wird.
- ☐ Ich kann beim One-Time-Pad begründen, warum es (bei perfekter Zufälligkeit, einmaliger Verwendung und gleicher Länge wie der Klartext) perfekte Sicherheit bietet (Schlüsselraum = Nachrichtenraum, Gleichverteilung der möglichen Klartexte).
- ☐ Ich kann die Anzahl möglicher OTP-Schlüssel einer gegebenen Länge berechnen (z.B. 26^n für Buchstaben, 2^n für Bits).
- ☐ Ich kann erklären, warum die Wiederverwendung eines OTP-Schlüssels zu Informationsleckage

führt und ein Beispiel analysieren.

- ☐ Ich kann die binäre Version des OTP (Bitweise XOR) anwenden und Kryptotexte berechnen.
- ☐ Ich kenne die Eigenschaften der XOR-Operation: Kommutativität, Assoziativität, neutrales Element 0, Involution (selbstinverse: $a \oplus a = 0$, $a \oplus 0 = a$) und deren Bedeutung für Ver- und Entschlüsselung.
- ☐ Ich kann erläutern, warum zweimalige Anwendung desselben Schlüssels (mit XOR) den Klartext zurückgibt.
- ☐ Ich kann das Three-Pass Protocol (Schlüsseltausch mit drei Durchgängen) Schritt für Schritt durchführen und die beteiligten Nachrichten (k_A, k_{AB}, k_B) bestimmen.
- ☐ Ich kann erklären, warum das Three-Pass Protocol unsicher ist, wenn ein Angreifer alle drei Kryptotexte mitschneidet (Rekonstruktion von t durch XOR aller Nachrichten).
- ☐ Ich kann das Diffie-Hellman-Merkle-Schlüsseltauschverfahren mit kleinen Zahlen durchführen und den gemeinsamen Schlüssel berechnen.
- ☐ Ich kann das zugrunde liegende Sicherheitsprinzip von Diffie-Hellman (Schwierigkeit des diskreten Logarithmusproblems) erklären.
- ☐ Ich kann den Man-in-the-Middle-Angriff auf Diffie-Hellman beschreiben und erläutern, wie digitale Signaturen (z.B. RSA) Authentizität sicherstellen.
- ☐ Ich kann eine Nachricht mit RSA asymmetrisch ver- und entschlüsseln, indem ich ein Beispiel mit kleinen Zahlen durchführe.
- ☐ Ich kann den Unterschied zwischen symmetrischen und asymmetrischen Verfahren (z.B. Vigenère/OTP vs. RSA/Diffie-Hellman) erklären.

Abbildungsverzeichnis

Glossar

DHM Diffie-Hellman-Merkle. 40, 41

GGT Grösster Gemeinsamer Teiler. 44

OTP One-Time-Pad. 29–33, 42

RSA Rivest–Shamir–Adleman. 41, 43–46