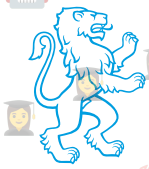


Kantonsschule Im Lee

Informatik

Kryptologie

Skript

Cyril Wendl

Inhaltsverzeichnis

Kapitel 1

Kryptologie

1.1 Einführung

Alice möchte Bob eine wichtige Nachricht zukommen lassen, beispielsweise zu einem gesundheitlichen Problem oder um ihre Bankkontoverbindung mit Bob zu teilen (s. **??**). Da das Internet jedoch eine *offene* und somit (grundsätzlich) unsichere Technologie ist, kann jedermann jede Nachricht mitlesen. Somit könnte eine bösartige Person, wie beispielsweise Eve, die Nachricht abhören, um sich Zugriff auf die Gesundheitsdaten oder das Bankkonto von Alice zu verschaffen.

Damit dies nicht passieren kann, muss Alice ihre Nachricht so verschlüsseln, dass nur Bob sie lesen kann. Dieses Problem hat sich bereits in der Antike (und vermutlich noch vorher gestellt) und entspricht einem grundsätzlichen, menschlichen Bedürfnis: Wie kann ein Feldherr seinen Soldaten Anweisungen geben, ohne dass der Gegner mithört? Oder, um eine andere Situation aufzugreifen: Wie können Sie sich mit Ihren Geschwistern austauschen, ohne dass Ihre Eltern verstehen, worum es geht?

In der Informatik spricht man hier davon, dass Alice aus ihrem „Klartext“, also dem für alle Menschen verständlichen Text, einen „Kryptotext“ macht, also einen Text, den nur Bob entschlüsseln kann, d.h., nur Bob weiss, wie man aus diesem Text wieder einen verständlichen Text macht. Hierzu muss man sich auf eine Verschlüsselungsmethode einigen. In der Informatik spricht man hierbei von einem **Verschlüsselungs-Algorithmus** und **Entschlüsselungs-Algorithmus**. Die Methode, um eine Nachricht zu verschlüsseln, so dass sie für Dritte unlesbar ist, wird häufig auch „**Schlüssel**“ genannt, und das Verfahren, um eine Nachricht unlesbar zu machen „Verschlüsselung“ oder „Chiffrierung“. Im Allgemeinen wird der Bereich der Informatik, der sich mit Ver- und Entschlüsselung befasst, „Kryptografie“ genannt und die verschiedenen Algorithmen und Ansätze werden häufig als „Kryptosysteme“ bezeichnet.

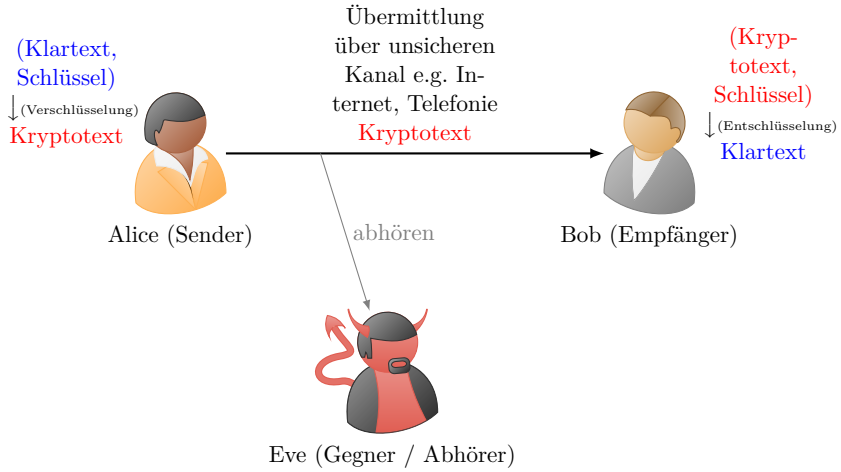


Abbildung 1.1: Dieses Schema zeigt die Kommunikation zwischen Alice (Sender) und Bob (Empfänger) unter Verwendung eines Kryptosystems.
ig:schema$_g$*eheimtext*

Im Folgenden setzen wir uns zuerst mit einigen grundlegenden Verschlüsselungs-Methoden auseinander, um zu verstehen, was ein sicheres Kryptosystem auszeichnet. Der niederländische Kryptologe und Linguist Auguste Kerckhoffs stellte im Jahr 1883 sechs Grundsätze für sichere Verschlüsselungsverfahren auf:

Abbildung 1.2: Auguste Kerckhoffs (1835-1903)
ig:kerckhoffs

1. Das System muss **unentzifferbar** sein.
2. Das System darf **keiner Geheimhaltung** bedürfen.
3. Das System muss **leicht übermittelbar** sein und man muss sich die **Schlüssel ohne schriftliche Aufzeichnung merken** können.
4. Das System sollte **mit telegraphischer Kommunikation kompatibel** sein.
5. Das System muss **transportabel** sein und die Bedienung darf nicht mehr als eine Person erfordern.
6. Das System muss **einfach anwendbar** sein.

Ein System, das diese Anforderungen erfüllt, gab es damals nicht. Von besonderer Wichtigkeit war

seine Forderung nach Öffentlichkeit des Kryptosystems:

> „Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi." – Auguste Kerckhoffs, *La cryptographie militaire* (1883)

Demgegenüber steht die Auffassung, dass Kryptosysteme geheimgehalten werden sollten (*Security through Obscurity*), eine Haltung, die häufiger von militärischen Institutionen sowie kommerziellen Anbietern von Verschlüsselungsmethoden verfechtet wird.

Folgende Sicherheits-bezogenen Anforderungen können zusätzlich an moderne Kryptosysteme gestellt werden:

1. **Vertraulichkeit**: Es soll sichergestellt sein, dass wirklich nur diejenige Person eine Nachricht lesen kann, für die diese bestimmt ist.
2. **Integrität**: Der Empfänger soll feststellen können, ob die Nachricht nach ihrer Erzeugung verändert wurde (wir wollen ja die originale Nachricht!).
3. **Authentizität**: Die Verfasserin einer Nachricht soll identifizierbar sein, bzw. der Empfänger soll nachprüfen können, wer die Verfasserin ist.
4. **Verbindlichkeit**: Die Verfasserin soll nicht abstreiten können, dass sie die Verfasserin der Nachricht ist.

1.2 Symmetrische Kryptosysteme

1.2.1 Verschlüsselung per Transposition

In einem mit Transposition (oder Permutation) verschlüsselten Text bleiben die Buchstaben des Klartexts im Kryptotext erhalten, ändern aber die Reihenfolge.

Aufgabe 1.1

Entziffern Sie den folgenden Kryptotext durch ausprobieren:

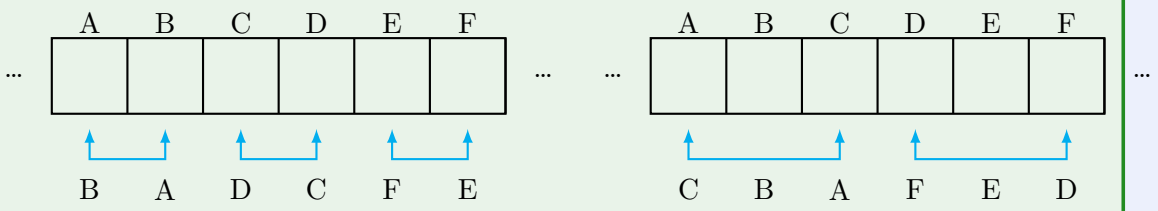
1. RKPYOTOLIGEEMREOLGCITHEGEHMIINSSE
2. HCSFIRILTAHCZFUEBUHAWNERDNUKUZMMOINUEIZNER

✔ Lösungsvorschlag zu Aufgabe 1.1

Ursprünglicher Text:

1. KRYPTOLOGIE ERMOEGLICHT GEHEIMNISSE
2. SCHRIFTLICH AUFZUBEWAHREN UND ZU KOMMUNIZIEREN

Der Kryptotext entsteht durch Austauschen der Positionen der Buchstaben, wie gezeigt in **??**.



(a) „Zweiertausch“ (b) „Dreiertausch“

Abbildung 1.3: „Zweiertausch“ und „Dreiertausch“
ig:transposition-cipher

1.2.2 Skytale

Das Kyrptosystem *Skytale* wurde bereits von den Griechen für militärische Zwecke verwendet. Der Verschlüsselungsalgorithmus kann wie folgt beschrieben werden:

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

Praktisch umgesetzt werden kann dieser Algorithmus mit einem Stab und einem Band, siehe **??**. Die Anzahl Zeichen, die auf eine Windung des Bandes um den Stab passen, entspricht der Anzahl Zeilen in der Tabelle. Diese Anzahl, also die Anzahl Zeilen, entspricht dem Schlüssel des Skytale-Verschlüsselungsverfahrens.

Abbildung 1.4: Praktische Umsetzung der Skytale-Verschlüsselung mit einem Stab und einem Band
Quelle

ig:skytale-band

Aufgabe 1.2

Der Kryptotext

WNGIAEIEMATSMKRTTEAGIEINANINTUGNDOJEEENL

wurde mit einer Tabelle mit 5 Zeilen und 8 Spalten erzeugt. Wie lautet der Klartext?

Lösungsvorschlag zu Aufgabe 1.2

Wir beginnen mit einer leeren 5×8 Tabelle und schreiben den Kryptotext spaltenweise (von rechts nach links und von oben nach unten) in die leere Tabelle. Damit erhalten wir:

W	E	T	T	I	N	G	E
N	I	S	T	E	I	N	E
G	E	M	E	I	N	D	E
I	M	K	A	N	T	O	N
A	A	R	G	A	U	J	L

Der Klartext

Wettingen ist eine Gemeinde im Kanton Aargau

lässt sich nun einfach ablesen.

Aufgabe 1.3

Der folgende Kryptotext der Länge 75 wurde mit SKYTALE verschlüsselt:

ETIFIITNUTNFGENKURRELEODIERSILIMSEANIE
MRECREMRHSNSSAPSTCBRCRHEUHORRNHNIEGEG

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

1. Welches ist hier der Schlüssel, d.h. die Anzahl Zeichen auf einer Windung (bzw. Anzahl Zeilen der Tabelle)? Tipp: Probieren Sie die Schlüssel 3 und 5 aus. Sie können diesen Link dazu verwenden.
2. Wie lautet der Klartext?
3. Wie viele Schlüssel müssen im schlimmsten Fall ausprobiert werden, bis der korrekte Schlüssel gefunden wurde? Das heisst, wie viele potentielle Schlüssel gibt es? Es gilt immer noch, dass alle Zeilen der Tabelle vollständig befüllt waren.

✔ Lösungsvorschlag zu Aufgabe 1.3

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

1. Durch Ausprobieren finden wir, dass die Wahl des Schlüssels 5 zu einem sinnvollen Klartext führt, die Wahl des Schlüssels 3 jedoch nicht.
2. Der Klartext lautet also:
   EIN KLEINER SCHRITT FUER MICH ABER EIN GROSSER SPRUNG FUER DIE MENSCHHEIT NEIL ARMSTRONG
3. Wir müssen $75 = 3 \cdot 5 \cdot 5$ Buchstaben auf ein Rechteck verteilen. Damit könnten $3, 5, 15$ und 25 mögliche Schlüssel sein. 1 und 75 sind keine Schlüssel, da der gegebene Text kein Klartext ist.

🏆 Aufgabe (Challenge) 1.4

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

✔ Lösungsvorschlag zu Aufgabe 1.4

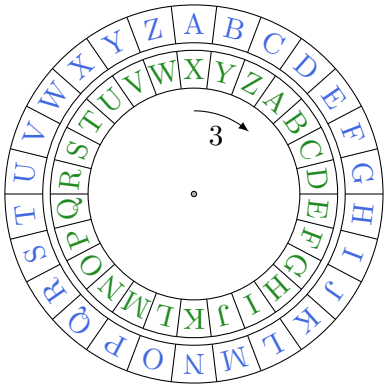
Die Tabelle benötigt 9 Spalten. Allgemein lässt sich die Anzahl benötigter Spalten berechnen durch

$$\left\lceil \frac{\text{Länge des Textes}}{\text{Anzahl Zeilen}} \right\rceil$$ (“ $\lceil ... \rceil$ ” bedeutet “nach oben aufgerundet”).

1.2.3 Caesar

Eines der bekanntesten Verschlüsselungssysteme der Antike ist die Caesar-Verschlüsselung, die von Julius Caesar verwendet wurde. Dieses Verschlüsselungssystem besteht essentiell aus einer Verschiebung aller Buchstaben um eine vordefinierte Anzahl Positionen im Alphabet. Der ***Schlüssel*** bezeichnet dabei die Anzahl Positionen, um die jeder Buchstabe verschoben wird. Ausgedrückt wird der Schlüssel auch als Buchstabe, der dem Buchstaben A entsprechen würde.

Beispiel 1.1:
Mit dem Schlüssel “D” (3 Positionen) würde das Wort “HALLO” als “KDOOR” geschrieben:



Der Schlüssel “B” bedeutet also eine Verschiebung um 1 Position, “C” um 2 Positionen, “D” um drei Positionen usw. Im Allgemeinen lässt sich die Verschiebung folgendermassen schreiben:

Verschiebung = Ord(□), wobei Ord(A) = 0.

Beispiel 1.2:
Folgender Text wurde mit dem Schlüssel “G” (6 Positionen) verschlüsselt:

```
  Klartext: JEMANDMUSSTEJOSEFKVERLEUMDETHA...
 Schlüssel: GGGGGGGGGGGGGGGGGGGGGGGGGGGGGG...
Kryptotext: PKSGTJSAYYZKPUYKLQBKXRKASJKZNG...
```

Aufgabe 1.5

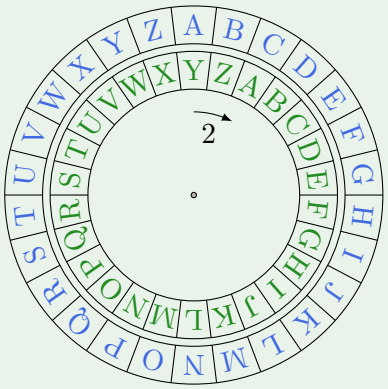
Der Kryptotext

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.

Lösungsvorschlag zu Aufgabe 1.5

Der häufigste Buchstabe im Kryptotext ist “G” Wir können den Text mithilfe der folgenden Verschiebung entschlüsseln (G → E) :



V E R W E N D E D E N S C H L U E S S E L Z W E I

1.2.3.1 Knacken von Caesar

- Einerseits reicht es, alle 25 möglichen Verschiebungen auszuprobieren. Ein moderner Computer hat dies in einigen Milisekunden erledigt.
- Andererseits kann, wenn der Text genügend lange ist, anhand der Häufigkeit der verschlüsselten Buchstaben mittels Häufigeitsanalyse in kürzester Zeit bestimmt werden, was der Schlüssel war. **??** zeigt die Häufigkeiten der Buchstaben eines langen, mit Caesar verschlüsselten Texts im Kryptotext.

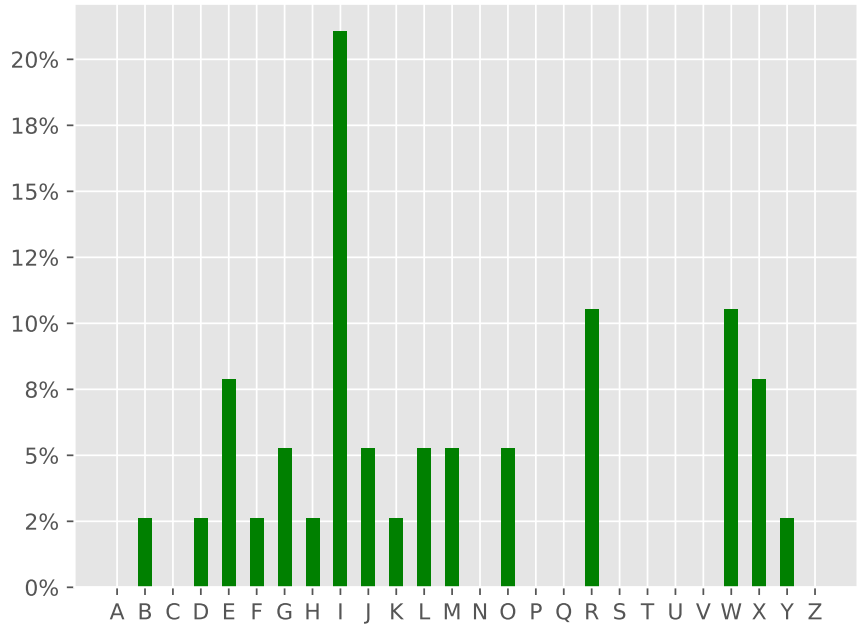


Abbildung 1.5: Buchstabenhäufigkeit in einem nach Caesar verschlüsselten Text
ig:caesar-freq

Die durchschnittlichen Häufigkeiten von Buchstaben, Bi- und Tri-Grammen in deutschen Texten ist in **??** 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 ab:buchstaben-haeufigkeitub@tab:buchstaben-haeufigkeit

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 ab:bigramme-haeufigkeitub@tab:bigramme-haeufigkeit

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 ab:trigramme-haeufigkeitub@tab:trigramme-haeufigkeit

Tabelle 1.1: Relative Häufigkeiten der Buchstaben, Bigramme und Trigramme im Deutschen ab:alle-haeufigkeiten

Aufgabe 1.6

Können Sie aus **??** und aus **??** entschlüsseln, was der Klartext ist?

Kryptotext:

`WMILEFIRIWKIWGLEJJXHMIWIRXIBXDYOREGOIR`

Lösungsvorschlag zu Aufgabe 1.6

Offensichtlich ist der häufigste Buchstabe im Kryptotext “I” und der häufigste Buchstabe in deutschen Texten ist der Buchstabe “E”, wir haben hier also vermutlich eine Verschiebung von “E” zu “I”, also eine Verschiebung um 4 Stellen. Der Klartext lautet daher: `SIEHABENESGESCHAFFTDIESENTEXTZUKNACKEN`

Aufgabe (Challenge) 1.7

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

Lösungsvorschlag zu Aufgabe 1.7

Falls der Text zu kurz ist, funktioniert die Häufigkeitsanalyse nicht immer, da der häufigste Buchstabe im Originaltext nicht immer der Buchstabe "E" ist. Dies wird beispielsweise im Wort "Wort" illustriert, das keinen Buchstaben "E" enthält. In diesem Fall müsste man alle 26 möglichen Verschiebungen durchprobieren.

Aufgabe (Challenge) 1.8

Um zu verschlüsseln, liest man die Caesar-Scheibe 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?

Lösungsvorschlag zu Aufgabe 1.8

Ja, dies tritt bei Schlüsseln 0 (A, keine Verschlüsselung) und 13 (N, die Hälfte des Alphabets) auf.

1.2.4 Monoalphabetische Substitution

Eine Weiterentwicklung der Caesar-Veschlüsselung besteht darin, nicht jeden Buchstaben im Klartext um dieselbe Anzahl Positionen zu verschieben, sondern für jeden Klartext-Buchstaben B_K einen Kryptotext-Buchstaben B_G zu definieren, durch den der Buchstabe ersetzt wird (s. **??**).

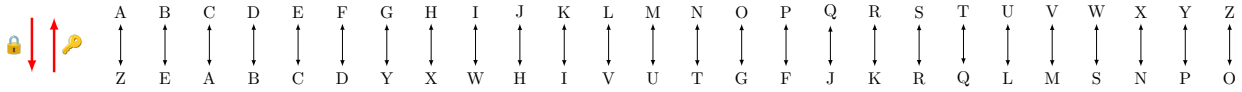


Abbildung 1.6: Monoalphabetische Substitution
ig:monoalph-subst

Diese Verschlüsselungsmethode kann nicht geknackt werden, indem alle Buchstaben um gleich viele Positionen verschoben werden. Man kann also nicht lediglich alle 25 möglichen Verschiebungen ausprobieren.

Obschon es nun eine Vielzahl möglicher Schlüssel gibt, kann diese Verschlüsselungsmethode ebenfalls sehr einfach geknackt werden per Häufigkeitsanalyse, die wir bereits in Unterabschnitt 1.2.3 gesehen und in Aufgabe 1.6 mittels **??** durchgeführt haben.

Beispiel 1.3:
Folgender Kryptotext wurde abgefangen:
`MUMMUXJUQYMHQOUSUTUQNGWTJQVHUMXQUXQJSUVYPPUM`

Wir wissen, dass er per monoalphabetische Verschlüsselung erstellt wurde, wie beispielsweise in **??**, kennen jedoch den Schlüssel nicht. Wir verwenden **??**, 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, Q kommt 6-mal vor. Aufgrund von **??** 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
  ```
- 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 **??** ist ein häufiges Trigramm in deutschen Texten ``DIE''. Dieses probieren wir einzusetzen (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.

Aufgabe 1.9

Entschlüsseln Sie den Text "ECRRCKZVRAZCRZK" mit dem Schlüssel aus **??**.

Lösungsvorschlag zu Aufgabe 1.9

BESSERALSCAESAR

Aufgabe (Challenge) 1.10

Lösen Sie eine Knobelaufgabe aus dem Kapitel "Substitution".

Aufgabe (Challenge) 1.11

Wie viele Verschlüsselungs-Möglichkeiten gibt es in der Verschlüsselungsmethode aus **??**?

Lösungsvorschlag zu Aufgabe 1.11

Für jeden Buchstaben gibt es 26 mögliche Verschiebungen (keine Verschiebung ist auch eine Möglichkeit), also gibt es insgesamt 26^{26} mögliche Verschiebungen.

1.2.5 Vigenère

Wie wir in Aufgabe 1.6 gesehen haben, ist es extrem einfach, Text, die mit Caesar verschlüsselt worden sind, anzugreifen, entweder mittels Buchstabenhäufigkeitsanalyse oder indem man einfach alle 25 möglichen Verschiebungen ausprobiert. Auch weitere monoalphabetische Substitutions-Verfahren wie **??** können durch etwas Knobeln relativ einfach geknackt werden.

Vigenère hatte eine andere Idee: Statt den ganzen Text mit einem einzigen Schlüssel zu verschlüsseln, verwendete er ein Wort, mit welchem er den Text "zyklisch", also gruppenweise verschlüsselte.

Beispiel 1.4:
x:vigenere Wenn der Schlüssel beispielsweise "KEY" war, wurden die Buchstaben folgendermassen verschlüsselt (s. Beispiel unterhalb):

- Buchstaben 1, 4, 7, 10 etc. mit "K"
- Buchstaben 2, 5, 8, 11 etc. mit "E"
- Buchstaben 3, 6, 9, 12 etc. mit "Y"

```
  Klartext: JEM|AND|MUS|STE|JOS|EFK|VER|LE...
 Schlüssel: KEY|KEY|KEY|KEY|KEY|KEY|KEY|KE...
Kryptotext: TIK|KRB|WYQ|CXC|TSQ|OJI|FIP|VI...
```

Im Vergleich dazu wird bei Caesar jeder Buchstabe durch *denselben* Schlüssel verschlüsselt, beispielsweise:

```
  Klartext: JEMANDMUSSTEJOSEFKVERLEUMDETHA...
 Schlüssel: GGGGGGGGGGGGGGGGGGGGGGGGGGGGG...
Kryptotext: PKSGTJSAYYZKPUYKLQBKXRKASJKZNG...
```

Wie Sie wissen, ist der Buchstabe "E" der häufigste Buchstabe in deutschen Texten. Diese Eigenschaft haben wir uns in Aufgabe 1.6 zunutze gemacht, um den Text zu knacken. Da bei Vigenère jedoch der Buchstaben nun nicht mehr immer mit demselben Schlüssel verschlüsselt ist, sondern je nach Position mit dem Schlüssel "K", "E", oder "Y", wird der Buchstabe "E" im Kryptotext nun breiter auf andere Buchstaben verteilt (s. **??**). Anders gesagt, ein Buchstabe im Kryptotext repräsentiert nun nicht mehr immer den gleichen Buchstaben im Klartext, sondern kann einen von drei Buchstaben repräsentieren.

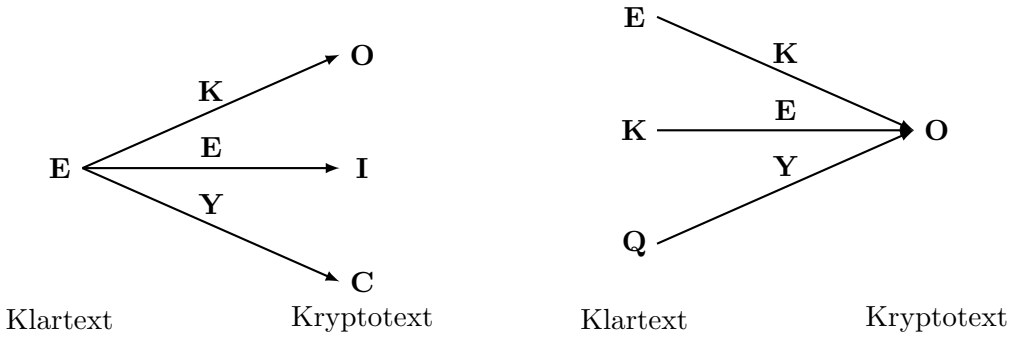
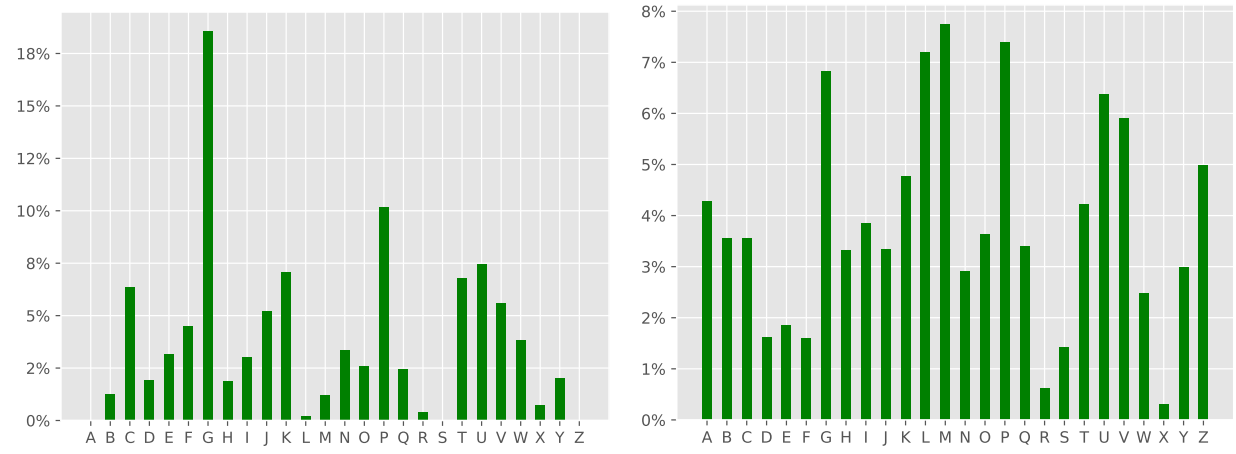


Abbildung 1.7: Verschlüsselungs-Möglichkeiten mit Vigenère, mit dem Schlüssel “KEY” aus **??**
ig:ex-vigenere-e

Diese Verschlüsslungsmethode galt während mehreren Jahrehunderten als sicher und war der Gold-Standard in vielen militärischen Verschlüsslungs-Anwendungen. Um einen Text zu verschlüsseln, wurde jeder Buchstabe im Klartext einzeln verschlüsselt, und je nach Schlüssel (z.B. “K”, “E” oder “Y” in **??**) wurde der entsprechende Buchstabe des Kryptotexts aus einer Tabelle herausgelesen (s. **??**)

?? zeigt die Buchstabenhäufigkeit im Kryptotext für einen langen Text, welcher einmal mit Caesar und einmal mit Vigenère verschlüsselt wurde.



(a) Caesar (b) Vigenère

Abbildung 1.8: Buchstabenhäufigkeit in einem langen Text, welcher mit unterschiedlichen Verfahren verschlüsselt wurde

ig:langer-text-vig-caesar

?? zeigt, dass Vigenère zu einer insgesamt homogeneren Verteilung aller Buchstaben im Kryptotext führt. Dies kommt daher, dass bei Vigenère jeder Klartext-Buchstaben auf *mehrere* Kryptotext-Buchstaben verteilt wird, währenddem bei Caesar jeder Klartext-Buchstaben durch genau *einen* Buchstaben im Kryptotext kodiert wird..

Klartextbuchstabe \ Schlüsselbuchstabe	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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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 1.2: Vigenère-Tabelle
ab:vigenere

Aufgabe 1.12

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`

Lösungsvorschlag zu Aufgabe 1.12

`BRAVOGUTGEMACHT`

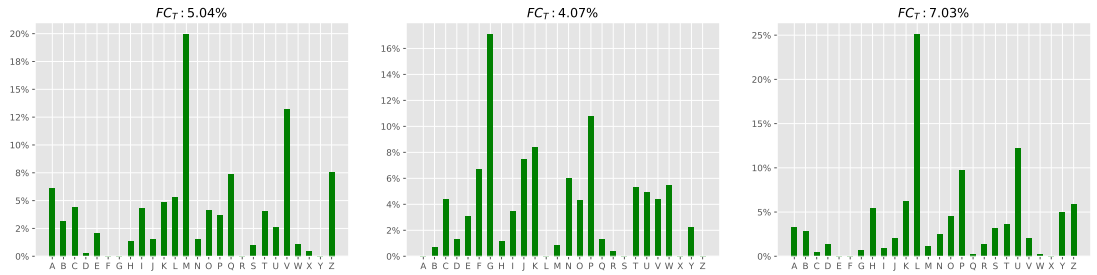
1.2.5.1 Knacken von Vigenère

Wenn die Schlüssellänge eines mit Vigenère verschlüsselten Texts bekannt ist, ist dieser relative einfach zu knacken: Man unterteilt den Text in diesem Fall einfach in Gruppen und geht für jede Gruppe gleich vor wie bei Caesar, um den Schlüssel zu finden.

Beispiel 1.5:
Angenommen, wir wüssten, dass folgender Text mit einem Schlüssel verschlüsselt worden ist, der drei Zeichen lang 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

Den Schlüssel selbst kennen wir nicht, wir wissen jedoch, dass jeder der grün markierten Buchstaben beispielsweise mit demselben Buchstaben verschlüsselt worden ist. Wir können also für jede der Gruppen (grün, blau, rot) die Häufigkeit der Buchstaben betrachten (s. **??**).

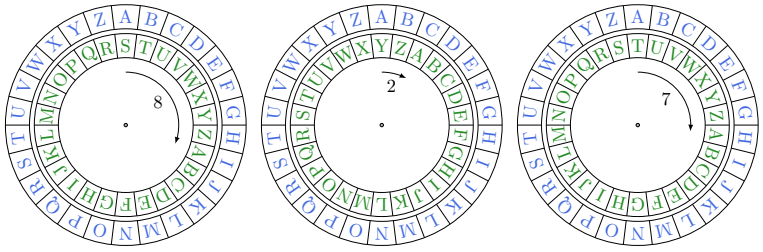


(a) Untergruppe 1 (b) Untergruppe 2 (c) Untergruppe 3

Abbildung 1.9: Buchstabenhäufigkeit in einem mit Vigenère verschlüsselten Text, pro Untergruppe

ig:vig-subgroup

Dabei erkennen wir, dass die häufigsten Buchstaben pro Gruppe M, G, bzw. L sind. Wir haben es also mit folgenden Verschiebungen zu tun:



Der Schlüssel muss demnach “ICH” sein und wir können den Text somit entschlüsseln.

Aufgabe 1.13

Versuchen Sie, den obigen Text mit dem Schlüssel "ICH" zu entschlüsseln, in dem Sie das Analysetool verwenden.

Lösungsvorschlag zu Aufgabe 1.13

```
ESSCHEINTOHNEFRAGEDASSSIEPERFEKTVERSTANDENHABENWIEMANVIGENEREENTSCHLUESS
ELTHERZLICHEGRATULATIONDAFU
```

Aufgabe 1.14

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.

```
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
```

Lösungsvorschlag zu Aufgabe 1.14

Mit dem Schlüssel "`OHA`" kommen wir auf folgende Lösung:

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

1.2.5.2 Bestimmung der Schlüssellänge: Friedman'sche Charakteristik

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, kann die Friedman'sche Charakteristik verwendet werden, um diese zu erraten.

Die Friedman'sche 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. Die effektive Häufigkeit eines Buchstaben hängt jedoch vom Buchstaben ab, wie wir in **??** gesehen haben. Die Häufigkeit des Buchstabens "E" in deutschen Texten ist beispielsweise ca. 17.4%. Die Häufigkeit eines Buchstabens $\square$ in einem Text T nennen wir $h_\square(T)$.

Die Friedman'sche Charakteristik berechnet, wie ungleich alle Buchstaben in einem Text verteilt sind, indem sie die Abweichung jedes Buchstabens von 1/26 berechnet und quadriert, um negative Werte zu vermeiden. Diese Abweichungen werden danach alle aufsummiert (s. Gleichung (1.1)).

$$FC(T) = \left(h_A(T) - \frac{1}{26}\right)^2 + \left(h_B(T) - \frac{1}{26}\right)^2 + \ldots + \left(h_Z(T) - \frac{1}{26}\right)^2 \tag{1.1}$$

$$= \sum_{\Delta \in \text{Alphabet}} \left(h_\Delta(T) - \frac{1}{26}\right) \tag{1.2}$$

Eine stark ungleiche Verteilung von Buchstaben in einem Text T führt also zu einer hohen Friedman'schen Charakteristik $FC(T)$, während dem gleichmässig verteiltere Buchstaben im Text T zu einer tieferen $FC(T)$ führen. Deutschsprachige (Klar-)Texte haben durchschnittlich etwa einen Wert von 3.8% (0.038) (s. **??**).

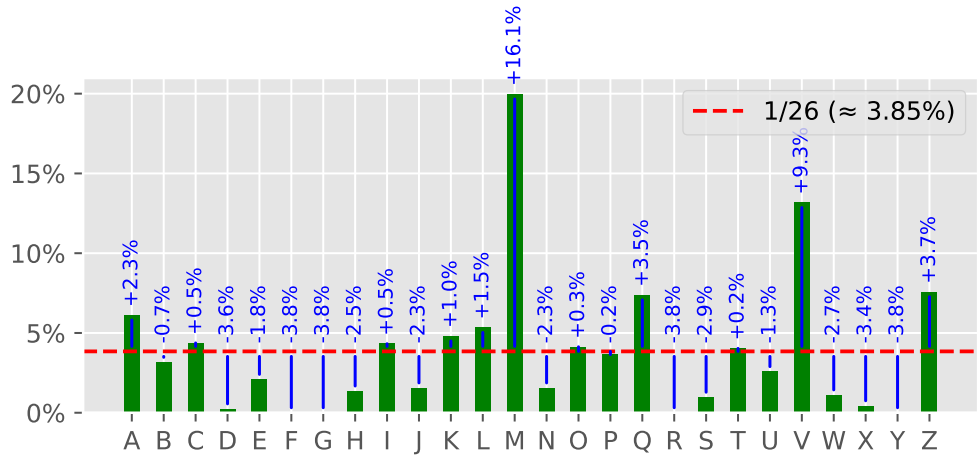


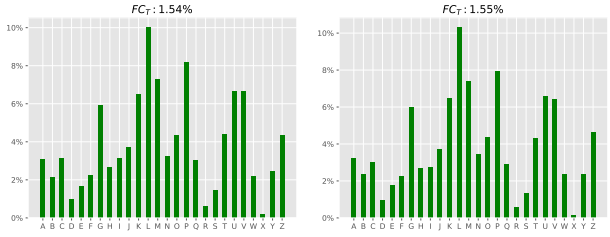
Abbildung 1.10: Buchstabenhäufigkeit in einem mit Caesar verschlüsselten Text, im Vergleich zur Gleichverteilung von Buchstaben

ig:vig-subgroup-1-avg

Je grösser die blauen Pfeile in **??**, desto höher die Friedman'sche Charakteristik.

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

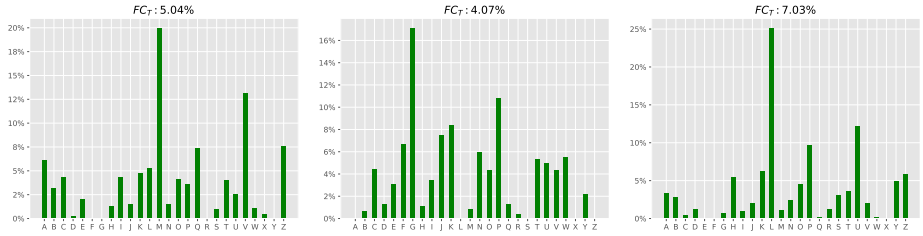
- Alle möglichen Schlüsselwortlängen von 1 bis zu einer beliebig gewählten Zahl n ausprobieren, wobei n praktisch nie über 10 gewählt wird.
- Buchstaben jeweils in Gruppen unterteilen:
  - **2 Gruppen**: MU ZK JL QP AW JU MH YI IL LC ZA UP MR LZ HL SV CM TZ BC UL GU PC IM PD QG TI PC QI LV GY MG UB UJ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



(a) Gruppe 1 (b) Gruppe 2

Abbildung 1.11: Buchstaben-Häufigkeiten und FC_T für Schlüsssellänge=2

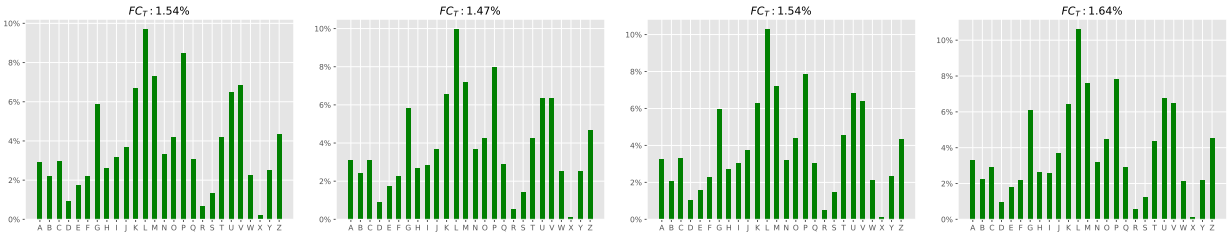
– **3 Gruppen**: MUZ KJL QPA WJU MHY IIL LCZ AUP MRL ZHL SVC MTZ BCU LGU PCI MPD QGT IPC QIL VGY MGU BUJ PNB MUZ MNA PGY HNP KJL OTH BWS IVP WPK IHB



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

Abbildung 1.12: Buchstaben-Häufigkeiten und FC_T für Schlüsssellänge=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 1.13: Buchstaben-Häufigkeiten und FC_T für Schlüsssellänge=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 durschschnittliche Friedman'sche Charakteristik für jede der getesteten Schlüssellängen ist gezeigt in **??**.

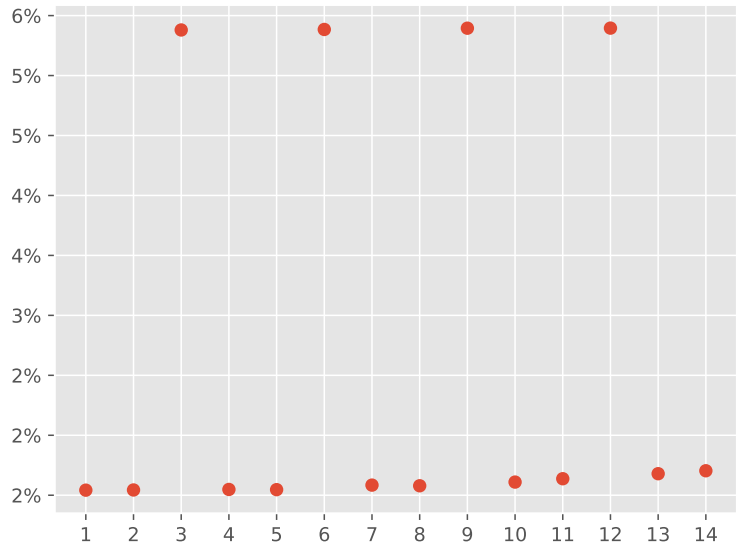


Abbildung 1.14: Durchschnittliche Friedman'sche Charakteristik für jede Schlüssellänge
ig:fc

Aus **??** lässt sich ablesen, dass die Schlüssellänge vermutlich 3 sein muss, da bei jedem Vielfachen der Schlüssellänge 3 die durchschnittliche Friedman'sche Charakteristik höher ist als für die restlichen Schlüssellängen. Ab nun lässt sich gleich vorgehen wie in Unterabschnitt 1.2.5.1 beschrieben, um den Text zu entschlüsseln.

Aufgabe 1.15

Berechnen Sie die Friedman'sche 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`

Lösungsvorschlag zu Aufgabe 1.15

Die Friedman'sche Charakteristik beträgt 29.5% und 7.3%, respektive. Wie sie sehen, ist die Friedmansch'e Charakteristik höher für Texte, bei denen jeder Buchstabe relativ häufiger vorkommt.

Aufgabe 1.16

Berechnen Sie die Friedman'sche 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 der ihrer Antwort? Wurde der Text mit Caesar oder mit Vigenère verschlüsselt?

✔ Lösungsvorschlag zu Aufgabe 1.16

Der tiefe Wert von 1.4% deutet darauf hin, dass der Text vermutlich mit Vigenère verschlüsselt wurde.

Aufgabe 1.17

Für welche Buchstabenverteilung sollte die Friedman'sche Charakteristik höher sein: **??**, (a) oder (b)?

✔ Lösungsvorschlag zu Aufgabe 1.17

$FC(T)$ sollte für **??** (a) höher sein, da die durchschnittliche relative Häufigkeit der Buchstaben im Kryptotext ungleicher ist.

Aufgabe 1.18

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

```
FZNZKVEDZFCRRZVFZTZFLVIOVBKMZWOVGVBAVSZSMVEDBHVNJAN
VNBZFZCCRFESPSTJEITSLECZJEGNAPIGZBEZEDQIDIOUBEZZAIV
RUSOXEIWFJSZWDYBDBBCLZWOLNYTSVUZAJTHHSJEENZFSEIGJED
DSTVRBSHVNYRJVFPSSJOGQIVSZSMVNBSTTHVTGVNDGUNIZRJVMZ
WOVIXVCZNNCHCUZQLCIXVNVIIPFJTZFTFGVBAZNYSNXEAIFYLZJ
PERPVJXEHRBJEDBWVRNIOBEIRBJSHSJEEFIOJTYOSLNOSSCEDRF
KIXVLFEIBUVJZHAKNDQIKZZWDYNZBOZCCHFZNZBTKRDQILNYPJE
NDSFZNBFPVSNSSVRHOMVRBSXVSZBBCSDBEZENSORUBSOSLDQLVN
RSOEDVGMZEWSURLPANZCCRBDPAHVEDYWFYOCSTFNISBEDZFPSEM
TMREXVFUEMIOUUMQIURDBHCIXVFEFDBTKEMBJJMZWOVSROMUENF
VYTPBEEUMSJEZZZOVSOFBYLZBTZCCWOUANWOEEMSIVIGWHKUHGU
VHGSOZCCRBENDAIFHZBHIANSBDFVZMVNYSOSAXVFCIZUFLNYBBV
HZFBEDZFFIDZHBLSZBEDAIBJXFVZUZGZUSRENQIVNHWSDEMYXLE
MRJXWZFEVNRSOEIXVERSRWNDEGBEVRFZFZNZBXVLONXZSXVFEHV
ZNVNYWFLNUOFYLDUFEUISSXRPSOULDQIVNBSTKAGHFEDZFXLEMA
DYEIRFIMPSDBCCSOEAZVFIAIAFZNZAIVRUSOWUZVMVUIRGLECZF
UIZUFXEIKBITYSTRLGABVCCHJXEIRFIUIGORCCGFZNZACZLYSTT
HPTERSRSIVNYSTRLGWFSEIRFEDZFVESDBFNIBSSNOIBFJCCKFSE
IRUIAZUULNYSSYAZZUDEDBGIEPBENEIBTUAIBVDMZWOVAPUFEDV
SNDEMHVEDYWFNEGHVDMDQIYEMIOUDZFIZMHSMXAINJEMZWOVRNS
FCEMIIEWDSEZEBSTKAGHFZNZFHVLDSCKEIRBENNSIEEDQIDIXVP
WTPBEUEIYFRCCYPVNIHFJTYIERSRWFUEMOVJDMIFTKZBLFEIBUV
SORVUEHDBGIZFFUANSJEHVIDYEIKBJSJJPCLNCXRRHWOUIMZFST
YOTJENKVVRYSEVRNDJVGZZEVIISSJEZZFNIZRFZNZGFVLZWTKDZ
FTGIZUFCDZGVEEIRMZCCSOXOOHFJMZWOWRZIOUAWSSZCCUFYEYO
SLEWSSQUBFVEDZWDYEMZJVGZIOKEMRFIGZKBCTYSSYEMFMZCCYF
```

```
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
```

✔ Lösungsvorschlag zu Aufgabe 1.18

Der Schlüssel lautet "`BRAVO`".

Aufgabe (Challenge) 1.19 Ver- und Entschlüsslung 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 diese mithilfe der Friedman'schen 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) 1.20

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

1.2.6 One-Time-Pad

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

1. Der Schlüssel besteht auf 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 1.6:
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 Friedman'schen 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.

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.

Aufgabe 1.21

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

Lösungsvorschlag zu Aufgabe 1.21

26^n.

1.3 Asymmetrische Kryptosysteme

In den bisher angeschauten Verschlüsslungsverfahren 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 un-praktikabel (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 kann, 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 (s. 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 (s. **??**). 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.

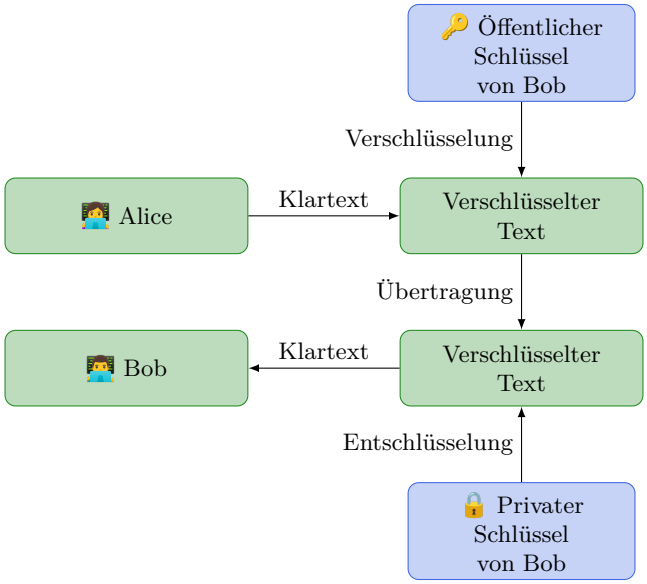


Abbildung 1.15: Prinzip der Public-Key-Verschlüsselung
ig:public-key-encryption

1.3.1 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.

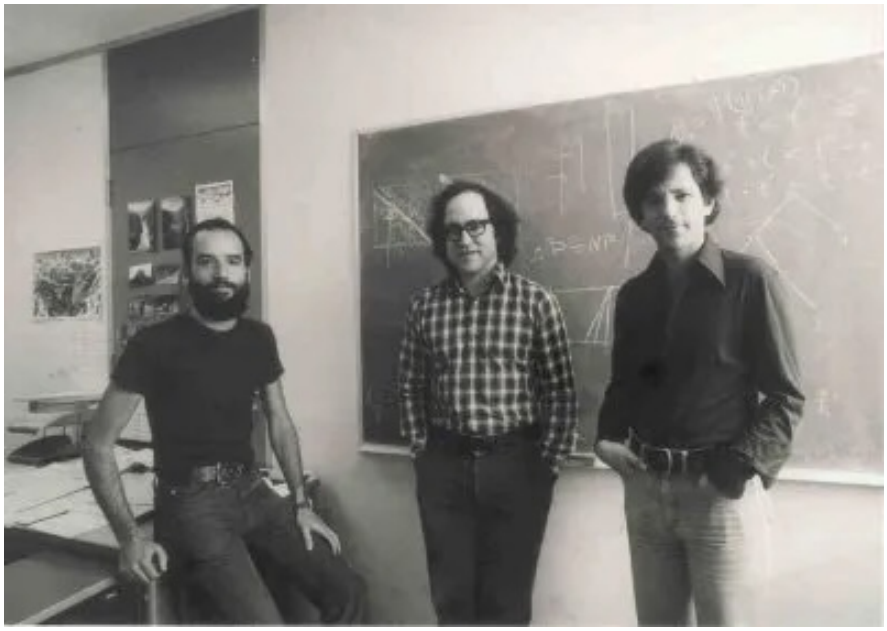


Abbildung 1.16: Ron Rivest, Adi Shamir und Leonard Adleman, die Erfinder des Rivest–Shamir–Adleman (RSA)-Verfahrens

ig:rsa

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 *Verschlüsslungsexponenten* 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 *Entschlüsslungexponenten* 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 1.7:
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 das Wort "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 1.22

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).

✔ Lösungsvorschlag zu Aufgabe 1.22

1. $n = p \cdot q = 5 \cdot 7 = 35$, $\varphi(n) = (p-1)(q-1) = 4 \cdot 6 = 24$.
2. Für e können wir beispielsweise 5 wählen, da 5 teilerfremd mit 24 ist.
3. $(5 \cdot d) \mod 24 = 1$. Dies finden wir beispielsweise mit $d = 5$.
4. Verschlüsselung:

$$\begin{aligned} c &= m^e \mod n \\ &= 9^5 \mod 35 \\ &= 4 \end{aligned}$$

.

5. Entschlüsselung:

$$\begin{aligned} m &= c^d \mod n \\ &= 4^5 \mod 35 \\ &= 9 \end{aligned}$$

Kapitel 2

One-Time-Pad und Schlüsseltausch

Der Fortschritt in der Mathematik und das dazu gekommene 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.

Vorgehen 2.1 (Kryptosystem ONE-TIME-PAD)**:**
yprocedure:onetime
Klartextalphabet: Alphabet der lateinischen Grossbuchstaben.
Kryptotextalphabet: Alphabet der lateinischen Grossbuchstaben.
Schlüsselmenge: Alle denkbaren Texte bestehend aus lateinischen Grossbuchstaben, welche dieselbe Länge haben wir 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 ONE-TIME-PAD 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 ONE-TIME-PAD geeinigt. Alice verwendet nun den mit Bob vereinbarten Schlüssel, um eine geheime Nachricht (Kryptotext) an ihn zu senden. Der gesendete Kryptotext lautet `GVRCL`.

Eva 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. Eva vermutet, dass der Kryptotext mit dem sicheren ONE-TIME-PAD verschlüsselt ist. Da der verwendete Schlüssel gleich lang ist wie der Klartext, ist eine Kryptoanalyse mit der Häufigkeitsanalyse unmöglich.

Aufgabe 2.1

(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?

Lösungsvorschlag zu Aufgabe 2.1

(a) Es gibt $26^5 = 11'881'376$ verschiedene Möglichkeiten.
(b) Selbst wenn sie alle Schlüssel ausprobieren würde, gäbe es viele Klartexte die denkbar wären. Alice könnte nicht wissen, welches der tatsächliche Klartext ist.

Dennoch hat Eva 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 Eva, dass sich Alice und Bob verabreden wollen. Eva 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 2.1: Entsprechende Schlüssel bei geratenen möglichen Klartexten (BADEN, ESSEN, LESEN, SPORT, VIDEO) für abgehörten Kryptotext GVRCL.
ab: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. Eva hat daher keine Möglichkeit herauszufinden, welche dieser vier möglichen Klartexte der geheimen Nachricht entspricht. Es ist auch möglich, dass der richtige Klartext nicht in der Liste steht. Somit hat Eva keine Chance irgendeinen Teil des Klartextes oder des Schlüssels zu erfahren.

2.1 Kryptoanalyse bei mehrfacher Verwendung des Schlüssels

Nun wollen wir wissen, weshalb ein Schlüssel beim ONE-TIME-PAD 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`.

Eva 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 Eva erneut nichts mit dem Kryptotext anfangen. Alice war jedoch nachlässig und verwendete den gleichen Schlüssel ein zweites Mal, um sich mit Bob zu verabreden. Eva 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 2.2: Entschlüsslung eines weiteren abgehörten Kryptotextes (ADRCM) durch die vorher bestimmten denkbaren Schlüsselkandiaten. Der Schlüsselkandidat FVOYY erzeugt aus beiden abgehörten Kryptotexten einen sinnvollen Klartext.

ab:ADRCM

Und siehe da, fast alle Texte in der dritten Spalte ergeben keinen Sinn, ausser dem Text in der ersten Zeile. Eva 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 Eva die tatsächlichen Klartexte und den Schlüssel herausfinden.

2.2 BIN-ONE-TIME-PAD

Das Kryptosystem BIN-ONE-TIME-PAD funktioniert fast gleich wie das ONE-TIME-PAD, 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 **??** wird im binären Alphabet die übersichtliche (binäre) VIGENÈRE-Tabelle:

Klartextbuchstabe \ Schlüsselbuchstabe	0	1
0	0	1
1	1	0

Abbildung 2.1: VIGENÈRE-Tabelle für das binäre Alphabet.
ig:VigenereBin

Der Tabelle entnehmen wir, dass der Klartextbuchstabe 0 durch den Schlüssel 0 zum Kryptotextbuchstaben 0 wird. Man verwendet für die Verschlüsslung mit der binären VIGENÈRE-Tabelle eine besondere Schreibweise. Für die Verschlüsslung 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 Verschlüsslung mit dem binären ONE-TIME-PAD 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 2.1:

- Der Klartext ist gegeben durch 101 und der Schlüssel durch 111. Dann ist der Kryptotext gegen 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 gegen durch

$$011101 \oplus 110001 = 101100.$$

Aufgabe 2.2

Berechnen Sie den Kryptotext zu dem gegebenen Klartext

$$110010100$$

und den Schlüssel

$$101110001.$$

Lösungsvorschlag zu Aufgabe 2.2

myexercise:0201 Der Kryptotext lautet

$$110010100 \oplus 101110001 = 011100101.$$

Aufgabe 2.3

(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?

Lösungsvorschlag zu Aufgabe 2.3

(a) Wir berechnen

$$100110 \oplus 001011 = 101101$$

sowie

$$001011 \oplus 100110 = 101101.$$

In beiden Fällen erhalten wir dasselbe Resultat.

(b) Es gibt lediglich die 4 Fälle, welche wir der binären VIGENÈRE-Tabelle entnehmen können. In den beiden Fällen $a = b = 0$ sowie $a = b = 1$ ist die Reihenfolge von a und b offensichtlich jeweils irrelevant, da sie identisch sind. In den beiden Fälle $a = 1$ und $b = 0$ sowie $a = 0$ und $b = 1$ gilt

$$a \oplus b = 1 \oplus 0 = 1 = 0 \oplus 1 = b \oplus a.$$

Damit sagt man, dass die Operation $\oplus$ *kommutativ* ist. Die Reihenfolge der Operanden spielt bei der Operation $\oplus$ keine Rolle.

Aufgabe 2.4

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

(a) Was macht die Verschlüsslung $a \oplus a$ 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 $a \oplus 0$?

Lösungsvorschlag zu Aufgabe 2.4

Mit Hilfe der binären VIGENÈRE-Tabelle begründen wir:

(a) $a \oplus a = 0$
(b) $a \oplus 0 = a$

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 2.5

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

$$k_A \oplus s_A$$

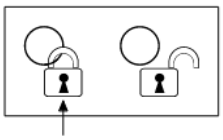
berechnet, also ihren Schlüssel erneut anwendet?

Lösungsvorschlag zu Aufgabe 2.5

Sie erhält den Klartext t zurück, denn

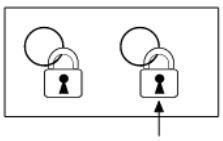
$$\begin{aligned} k_A \oplus s_A = \\ & (t \oplus s_A) \oplus s_A = \\ & t \oplus (s_A \oplus s_A) = \\ & t \oplus \underbrace{s_A \oplus s_A}_{=0} = \\ & t \oplus 0 = \\ & t. \end{aligned}$$

2.3 Schlüsseltausch



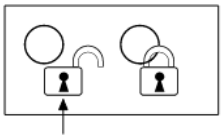
Absender schließt

	Klartext	101011
⊕	Absender-Schlüssel	011011
	Erster Krypto-Text	110000



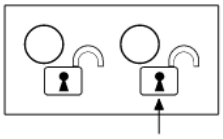
Empfänger schließt

	Erster Krypto-Text	110000
⊕	Empfänger-Schlüssel	101010
	Zweiter Krypto-Text	011010



Absender öffnet

	Zweiter Krypto-Text	011010
⊕	Absender-Schlüssel	011011
	Dritter Krypto-Text	000001



Empfänger öffnet

	Dritter Krypto-Text	000001
⊕	Empfänger-Schlüssel	101010
	Klartext	101011

Abbildung 2.2: Schlüsseltausch
ig:tausch

Vorgehen 2.2 (Kommunikationsprotokoll DIGITALER SCHLÜSSELTAUSCH)**:**
yprocedure:Komm

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 k_B:

$$t = k_B \oplus s_B$$

   und erhält dadurch den Klartext t, welchen ihn Alice wissen lassen 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 2.6

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

Lösungsvorschlag zu Aufgabe 2.6

An der Tafel.

2.4 Diffie-Hellman-Merkle-Schlüsseltausch

Vorgehen 2.3 (Protokoll DIFFIE-HELLMAN-MERKLE (DHM))**:**
myprocedure:Diffie

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 2.7

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.

Lösungsvorschlag zu Aufgabe 2.7

An der Tafel.

Aufgabe 2.8

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

Lösungsvorschlag zu Aufgabe 2.8

(a) $a = 2, b = 3$ und $s_{AB} = 3^{2 \cdot 3} \mod 5 = 4$
(b) $a = 5, b = 7$ und $s_{AB} = 2^{5 \cdot 7} \mod 13 = 7$

Kapitel 3

Lernziele Kryptologie

- ☐ Ich weiss wie die folgenden Kryptosysteme funktionieren (Verschlüsslung und Entschlüsslung bei gegebenem Schlüssel):
  - ☐ Skytale
  - ☐ Caesar
  - ☐ Vigenère
  - ☐ One-Time-Pad
  - ☐ RSA
- ☐ Ich kann die Verschlüsslung und Entschlüsslung mit Caesar und Vigenère in Python implementieren.
- ☐ Ich kann einen Kryptotext, der durch die Vigenère-Verschlüsslung entstanden ist, mit Hilfe des Tools auf folgender Webseite entschlüsseln:
  https://cryptbreaker.marcwidmer.xyz
- ☐ Ich kann die Idee der Häufigkeitsanalyse erklären.
- ☐ Ich kann eine gruppenweise Häufigkeitsanalyse durchführen, um Vigenère bei bekannter Schlüssellänge zu knacken.
- ☐ Ich kenne das Kerckhoff'sche Prinzip der Sicherheit.
- ☐ Ich kann die Friedman'sche Charakteristik für einen kurzen Text von Hand berechnen
- ☐ Ich kann mit der Friedman'schen Charakteristik die Länge eines Vigenère-Schlüssels bestimmen.
- ☐ Ich kann erklären, was mit der Friedman'sche Charakteristik berechnet wird.
- ☐ Ich kann eine Nachricht mit RSA asymmetrisch ver- und entschlüsseln, indem ich ein Beispiel mit kleinen Zahlen durchführe.