Kryptographie

Eine Einführung für die Verwendung in der Schule

von
Mathias Helbing, 2010 - 2019

Inhaltsverzeichnis

Das Problem von Alice und Bob

Alice und ihr Freund Bob schreiben sich gerne gegenseitig Briefe. Allerdings haben sie das Problem, dass Bobs kleiner Bruder Mallory ständig herum schnüffelt und gerne Post liest, die ihn nichts angeht. Deswegen möchten die beiden ihre Briefe so schreiben, dass Mallory nichts damit anfangen kann, wenn er sie findet.

Alice macht den Vorschlag, die Nachricht in einer Geheimschrift zu schreiben, so dass Mallory nur sinnlose Buchstaben zu lesen bekommt, während Alice und Bob genau wissen, wie sie die Geheimschrift wieder in echte Schrift übersetzen können.

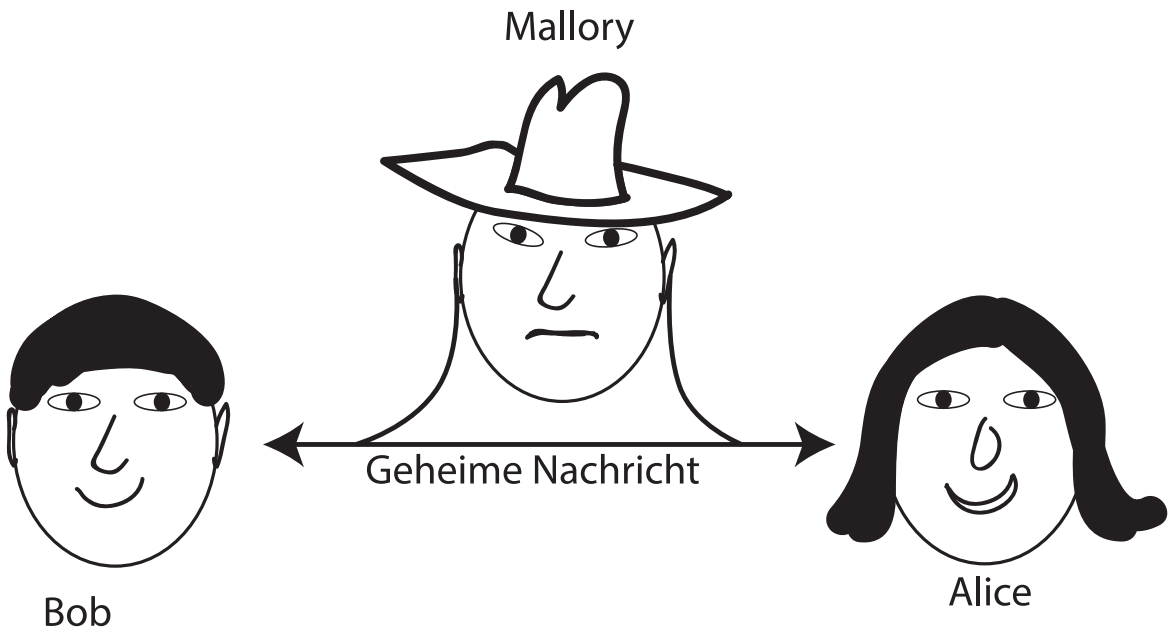
Aufgabe:

Kannst Du Alice und Bob eine Geheimschrift (oder auch mehrere) vorschlagen? Erstelle ein Poster oder eine Folie, worauf Du das Verfahren beschreibst.

Information:

Die Wissenschaft, die sich mit der Geheimhaltung von Informationen beschäftigt, nennt man **Kryptologie**. Sie umfasst die **Kryptographie** (das Schreiben von Geheimtexten) und die **Kryptoanalyse** (das „Knacken" von Geheimtexten).

Das „Alice/Bob/Mallory-Modell" wird in der Kryptologie sehr häufig verwendet. Mit Alice und Bob werden die beiden Personen bezeichnet, die sich gegenseitig geheime Nachrichten übermitteln wollen, während Mallory der „Bösewicht" ist, der die Nachricht unbefugt mithören oder gar unbemerkt verändern will; „Mallory" kommt vom englischen Wort „malicious", was „hinterlistig" oder „bösartig" bedeutet.



Auch der große Cäsar hatte seine kleinen Geheimnisse…

Bereits der römische Feldherr Julius Cäsar hat seine Nachrichten manchmal in Geheimschrift geschrieben, denn gerade im Krieg hängt der Erfolg häufig davon ab, dass man seine eigenen Pläne vor dem Feind geheim hält. Dabei wählte Cäsar eine recht einfache Methode: Er ersetze jeden Buchstaben seiner Nachricht durch den Buchstaben, der im Alphabet drei Stellen später kommt. Aus einem A wird ein D, aus einem B ein E usw. Da es nach den Buchstaben X, Y und Z keinen Buchstaben mehr gibt, fängt man einfach wieder bei A an.

Original	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
Geheim	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

Aus der Nachricht „angriff erfolgt um mitternacht“ wird also der scheinbar unsinnige Buchstabensalat „dqjulii huirojw xp plwwhuqdfkw“. Aber wenn man Bescheid weiß, dann ist das Entziffern kein Problem mehr.

Natürlich muss man die Buchstaben nicht um drei Stellen verschieben. Ebenso gut denkbar sind natürlich z. B. auch 7 Stellen oder 16 Stellen. Mithilfe einer Chiffrierscheibe (siehe Bastelbogen auf der nächsten Seite) können wir alle Möglichkeiten einstellen.

Aufgabe:

Verschlüssle mit der Methode von Cäsar Deinen Namen.

Was bedeutet „jxw jhpdfkw gx kdvw hv yhuvwdqghq“?

Ist die Methode von Cäsar ein gutes Verschlüsselungsverfahren? Kann man kleinere Dinge verändern, die das Verfahren besser machen?

Information:

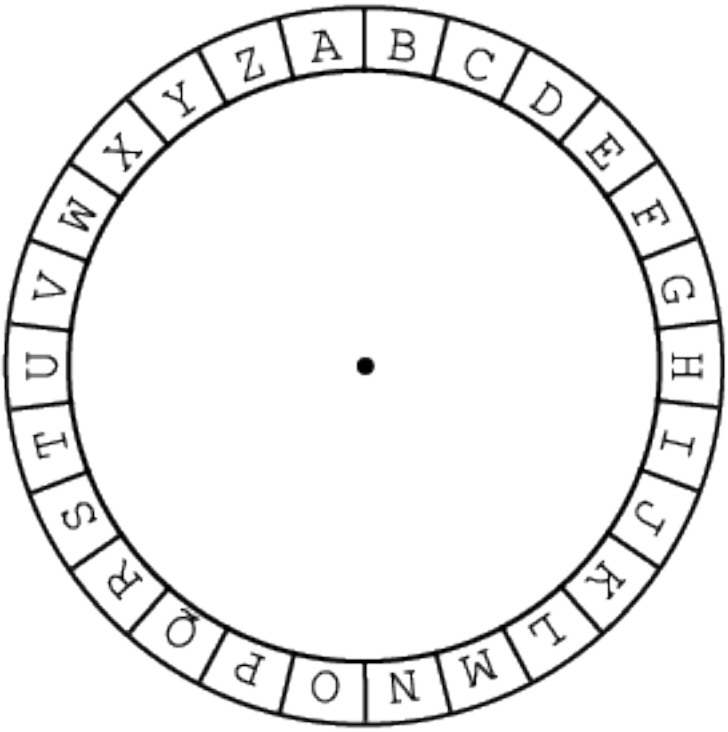
Die Nachricht, die man in Geheimschrift übersetzen will, heißt **Klartext**; jeder kann ihn lesen. Den Text in Geheimschrift nennt man dann **Geheimtext**. Die geheime Information, die man zum Verschlüsseln und Entschlüsseln benötigt, heißt **Schlüssel**.

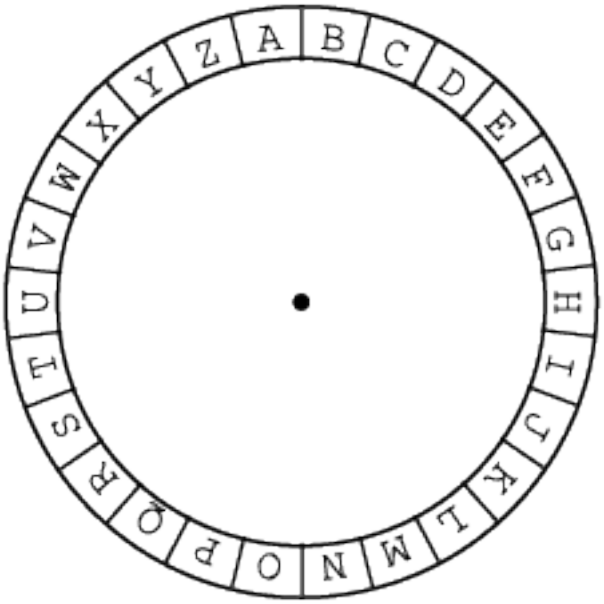
Eine Methode, um aus einem Klartext einen Geheimtext zu machen, nennt man Verschlüsselungsverfahren oder einfach Code.

Einen Text in Geheimschrift zu übertragen nennt man **verschlüsseln**, **chiffrieren** oder **codieren**. Das Zurückübersetzen in den Klartext nennt man **entschlüsseln**, **dechiffrieren** oder **decodieren**. Wenn ein Unbefugter einen Geheimtext entschlüsselt, dann sprechen wir vom **Knacken** oder **Brechen** des Codes.

Wir basteln eine Chiffrierscheibe

- Klebe die beiden Scheiben auf Pappe, und schneide die Scheiben danach aus.
- Stich in die kleine Markierung in der Mitte der Scheiben jeweils ein Loch und befestige die kleine Scheibe auf der großen mit einer Musterklammer.
- Erkläre, wie man diese Scheibe zum Verschlüsseln und Entschlüsseln benutzt.





Mallory knackt den Code

Neugierig wie immer schnüffelte Mallory in den Sachen seines Bruders herum. Zwischen den Comics fand er einen Brief, in dem er den folgenden Inhalt lesen konnte:

> qjuux kxk!
>
> fxuunw fra vxwcjp rwb trwx pnqnw? mna wndn qjaah yxccna oruv txvvc!
>
> padbb jurln

„Was soll der Quatsch denn bedeuten?", murmelte Mallory und wühlte etwas weiter. Sein Blick fiel auf eine Chiffrierscheibe, die Mallory ausführlich untersuchte.

Weil er ein pfiffiges Kerlchen ist, hatte Mallory aber schnell durchschaut, wie das System funktioniert, und nach wenigen Minuten des Probierens hatte er die richtige Einstellung der Scheibe gefunden und konnte den Brief ohne Mühe lesen.

Aufgabe:

1. Das kannst Du sicher auch, oder? Wie lautet der Klartext?
2. Wie viele mögliche Einstellungen der Scheibe muss Mallory im ungünstigsten Fall ausprobieren?
3. Angenommen, Mallory möchte Bobs Computerpasswort durch Ausprobieren herausfinden. Wie viele Möglichkeiten muss er probieren, wenn er weiß, dass das Passwort nur aus Kleinbuchstaben (a bis z) und Ziffern (0 bis 9) besteht und insgesamt 8 Zeichen hat? Wie lange braucht er, wenn er pro Sekunde ein Passwort probieren kann? Gib das Ergebnis in einer sinnvollen Zeiteinheit an.

Information:

Ein Verfahren, bei dem ein Buchstabe durch einen anderen ersetzt wird, heißt **Substitutionsverfahren**. „Substituieren" kommt aus dem Lateinischen und heißt „ersetzen".

Man kann jedes Verschlüsselungssystem knacken, wenn man alle möglichen Schlüssel ausprobiert. So etwas nennt man „brute force attack", was so viel wie „Angriff mit roher Gewalt" bedeutet. Bei der Chiffrierscheibe ist das nicht besonders viel Arbeit, aber bei guten Verschlüsselungssystemen ist die Anzahl der möglichen Schlüssel viel größer, so dass man (selbst mit Computerhilfe) nicht alle ausprobieren kann.

Aber Achtung! Wir werden noch sehr viel intelligentere Angriffe kennen lernen als das reine Ausprobieren aller Schlüssel. Deswegen ist eine große Zahl möglicher Schlüssel noch lange keine Sicherheitsgarantie, sondern nur eine (von vielen) Voraussetzungen.

Neue Ideen braucht das Land

Alice und Bob trauten ihren Augen nicht, als Mallory vor dem Kino auftauchte und ihnen triumphierend mitteilte, dass er die Geheimschrift ohne Probleme geknackt hatte. Er erklärte ihnen auch, wie er das schaffen konnte: Er hat einfach alle Möglichkeiten der Scheibe ausprobiert – das waren ja höchstens 25 und damit kein Problem.

Nach dem Film wollen Alice und Bob eine bessere Geheimschrift erfinden. Nach einigem Grübeln hatte Bob eine Idee: „Hm… die Scheibe hat 25 Möglichkeiten. Aber wenn wir die Reihenfolge der Buchstaben verändern, dann haben wir doch noch viel mehr!"

Alice verstand ihn zuerst nicht, aber Bob erklärte ihr das Ganze mit einer Tabelle:

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

„Die Idee ist ähnlich wie bei Cäsar. Aber wir ändern einfach die Reihenfolge des unteren Alphabetes! Und wenn wir dafür sorgen, dass Mallory die untere Reihenfolge nicht kennt, dann kann er auch mit Probieren nicht viel erreichen – es gibt ja unendlich viele Möglichkeiten!"

Alice hatte das System verstanden, fühlte sich aber unwohl: „Und wie merken WIR uns die Reihenfolge? Aufschreiben ist schlecht, denn dann findet dein Bruder den Zettel wahrscheinlich."

„Nichts leichter als das! Schau dir die Tabelle nochmal ganz genau an. Ich kann sie mir total leicht merken… oder zumindest jederzeit aus dem Kopf hinschreiben."

Aufgabe:

1. Wie ist der Trick, wie man sich die zufällige Anordnung der Buchstaben in der unteren Zeile merken kann?
2. Bob hat ja behauptet, dass es unendlich viele Möglichkeiten gibt. Stimmt das wirklich?
3. X, Y und Z werden in Bobs Tabelle nicht ausgetauscht. Ist das schlimm?

Information:

Natürlich kann man in die untere Zeile auch noch andere Dinge als Buchstaben schreiben. Wir könnten z. B. eine Tabelle der folgenden Art benutzen:

Original	A	B	C	D	…	X	Y	Z
Geheim	!	$	=	>	…	*	#	t

Dann gibt es tatsächlich so gut wie „unendlich" viele Möglichkeiten. Eine solche Verschlüsselung, bei der man das Alphabet durch ein anderes (oder durch dasselbe Alphabet in einer anderen Reihenfolge wie oben) ersetzt, heißt **monoalphabetische Verschlüsselung**. Wir werden später sehen, dass solche Verschlüsselungen relativ schwach und damit leicht zu brechen sind.

Mallorys nächster Angriff

Natürlich war Mallory sehr stolz auf sich, dass er den geheimen Brief lesen konnte. Er liebt es, wenn er zeigen kann, dass er mindestens so schlau wie sein älterer Bruder ist. Als er eines Tages mal wieder schnüffelte, fand er einen weiteren Brief, der dem ersten ziemlich ähnlich sah:

ueddi lil

unqpn pmnttnh wsm qho sh anm nsoasndn qg vsnm

rmqoo edsfn

Er holte seine Chiffrierscheibe hervor (er hatte sich natürlich eine gebastelt) und probierte alle möglichen Einstellungen aus. Aber wie er die Scheibe auch einstellte: Nie kam etwas Sinnvolles heraus. „Mist… da haben sich die Beiden wohl was Besseres einfallen lassen!", fluchte er. Aber das Wort „aufgeben" kennt Mallory nicht. Also schrieb er den Brief sorgfältig ab und zog sich auf sein Zimmer zurück, um etwas zu Grübeln…

Aufgabe:

Du hast Mallory gegenüber einen Vorteil, denn Du weißt ja, wie das System der beiden funktioniert. Den Schlüssel „Kuhwiesn" haben sie aber nicht verwendet, denn Alice hat Angst vor Kühen.

Findest Du eine Möglichkeit, den Text der beiden zu knacken?

Information:

Es ist ein großer Vorteil, wenn man das System kennt, mit dem ein Text verschlüsselt wurde. Deswegen ist die Aufgabe für Dich (etwas) leichter als für Mallory. Trotzdem versuchen Profis normalerweise nicht, ihre Systeme geheim zu halten, sondern nur den Schlüssel.

Das hat den Grund, dass ein bekanntes System von vielen Experten untersucht werden kann, so dass man viel schneller mögliche Schwächen findet. In der Vergangenheit war es so, das Erfinder ihre Systeme für sicher gehalten haben – aber im praktischen Einsatz wurden sie schnell geknackt, weil sie leider doch unsicher waren. Hätten vorher viele Experten das System untersuchen können, dann wäre das schlechte System gar nicht benutzt worden.

Der Kryptologe **Auguste Kerckhoffs** formulierte 1883 den heute noch gültigen Grundsatz: *„Die Sicherheit eines Verschlüsselungsverfahrens darf nur von der Geheimhaltung des Schlüssels abhängig sein und nicht von der Geheimhaltung des Verfahrens!*"

Das bedeutet: Auch wenn alle genau wissen, wie das Verfahren funktioniert, dürfen sie nicht in der Lage sein, einen Text zu knacken, wenn sie den Schlüssel nicht kennen.

Heutzutage versucht normalerweise niemand mehr, die Arbeitsweise der Verschlüsselungsverfahren geheim zu halten, im Gegenteil: Alle modernen Verfahren sind veröffentlicht und können von jedermann untersucht werden. So werden neben möglichen Schwächen auch eventuell absichtich eingebaute „Hintertüren" entdeckt, mit deren Hilfe sich der Code auch ohne Schlüssel dechiffrieren lässt.

Wenn man sich aber sicher ist, dass das eigene Verschlüsselungssystem Kerckhoffs' Prinzip erfüllt, dann kann man durch Geheimhalten der Arbeitsweise vielleicht noch ein bisschen mehr Sicherheit bekommen („security through obscurity"), da der Feind zunächst die Arbeitsweise des Verfahres herausfinden muss. Viele Geheimdienste haben solche geheimen Verfahren in der Hinterhand. Aber die haben auch genügend Experten, die die Verfahren untersucht und für sicher befunden haben. Auch wenn das Verfahren bekannt wird, kann es trotzdem nicht gebrochen werden.

Mallory knackt den Code

Mallory ist ziemlich pfiffig, das haben wir bereits erwähnt. Und so hatte er eine Reihe von Ideen, um den verbesserten Code von Alice und Bob zu knacken. Schnell hatte der Junge eine Vermutung: Wahrscheinlich wird er es auch hier wieder mit einer Buchstabenersetzung zu tun haben, aber sie wird nicht so „gleichmäßig" wie bei der Scheibe sein.

Mallory schaute sich den Text nochmals an.

ueddi lil
unqpn pmnttnh wsm qho sh anm nsoasndn qg vsnm
rmqoo edsfn

Bobs kleiner Bruder wurde nachdenklich: „Hm… dieser Anfang „ueddi lil" … das könnte doch ‚Hallo Bob' heißen, denn so fängt Alice ihre Briefe meistens an. Und außerdem unterschreibt sie ihre Briefe meist mit ‚Gruß' (oder Gruss) Alice'. Dann steht ‚u' für ‚h', ‚e' für ‚a' … „

Er notierte seine Vermutungen in einer Tabelle:

Original	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
Geheim	E	L	F		N		R	U	S			D			I			M	O		Q					

Also ersetzte Mallory alle Buchstaben, die er schon kannte. Das gab ihm Hinweise für weitere Worte, die er raten konnte.

Mit etwas Probieren (das muss man als Codeknacker häufig tun) hatte er schließlich die Tabelle vervollständigt, und er konnte den Text entziffern.

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

Mallory war zu recht ziemlich stolz auf sich, dass er diesen Code geknackt hatte.

Information:

Wenn man Teile des Klartextes kennt (oder erraten kann), dann ist es häufig sehr einfach, den restlichen Text zu knacken und den Schlüssel herauszufinden. Weil Mallory wusste (oder vermutet hatte) dass im Klartext „Hallo Bob" steht, hatte er einen guten Ansatzpunkt für seine Arbeit.

Auf diese Art wurden in der Vergangenheit viele Codes gebrochen (z. B. konnten die Engländer im zweiten Weltkrieg die Codes der Deutschen ähnlich knacken, auch wenn der Code viel komplizierter war). Solch eine Angriff, bei dem der Angreifer einen Teil des Klartextes kennt, nennt man in der Kryptologie „**known plaintext attack**" – oder auf Deutsch: „Angriff/Attacke mit bekanntem Klartext".

Viele der „klassischen Verfahren" bieten einem solchen Angriff nur wenig Widerstand und lassen sich (mehr oder weniger leicht) damit brechen. Eine verschärfte Form ist die „**chosen plaintext attack**". Hierbei kann der Angreifer selbst Klartexte (oder Teile davon) vorgeben und den Geheimtext bekommen. Dieses Szenario führt bei allen klassischen Verfahren dazu, dass der Angreifer den Schlüssel schnell ermitteln kann.

Tatsächlich ist ein solcher Angriff durchaus praktisch relevant. Man könnte im Krieg z.B. ein Minenfeld legen, dessen Position der Feind dann verschlüsselt übermittelt. Fängt man diese Nachricht ab, dann liegt in gewisser Weise eine „chosen plaintext attack" vor. In der Tat soll das britische Militär im 2. Weltkrieg so vorgegangen sein.

Moderne Verfahren sind so konstruiert, dass sie solchen Angriffen gut widerstehen.

Codeknacken mithilfe von Mathematik

Mallory konnte und wollte seinen erneuten Erfolg nicht für sich behalten, und er ließ seinen Bruder wissen, dass er den Code gebrochen hatte. Und er teilte Bob natürlich auch alle Details seines Vorgehens mit.

Eine gewisse Bewunderung konnte sich Bob nicht verkneifen, denn so viel Raffinesse hatte er seinem kleinen Bruder nicht zugetraut. Aber nun war natürlich erneuter Kriegsrat mit Alice angesagt, denn die beiden mussten einen neuen, noch besseren Code erfinden.

„Hm….. Mallory konnte unseren Code nur knacken, weil er gewisse Worte raten konnte. Was ist denn, wenn wir nur Worte benutzen, die er niemals erraten kann?", fragte Alice.

„Das ist ganz schön schwierig!", antwortete Bob. „Ohne ein paar Standardwörter kommt man wohl kaum aus. Und außerdem habe ich mich schlau gemacht. Es würde nicht viel bringen, wenn Mallory nichts erraten könnte. Denn er hätte noch auf eine andere Art unseren Code knacken können."

„Wie denn?", wollte Alice wissen.

„In der deutschen Sprache kommt der Buchstabe ›E‹ sehr viel häufiger vor als jeder andere Buchstabe. Wenn Mallory also schaut, welcher Buchstabe in unserem Geheimtext besonders oft vorkommt, dann hat er das „E" gefunden. Und genauso kann er es mit dem zweithäufigsten Buchstaben (das ist das „N") machen und so weiter. Und auch wenn wir die Buchstaben durch Symbole ersetzen hilft uns das nicht, weil das Prinzip das gleiche ist."

„Echt? Klappt das immer?"

„Naja… so ganz perfekt kommt es meistens nicht hin, denn es kann ja sein, das in unserem Klartext zufällig nur wenige „E" vorkommen und dafür zum Beispiel das „R" häufiger ist. Aber mit etwas Probieren kriegt man das schnell raus. Im Internet gibt es eine Tabelle mit den Buchstabenhäufigkeiten."

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 %
L	3,44 %
C	3,06 %
G	3,01 %
M	2,53 %

O	2,51 %
B	1,89 %
W	1,89 %
F	1,66 %
K	1,21 %
Z	1,13 %
P	0,79 %
V	0,67 %
ß	0,31 %
J	0,27 %
Y	0,04 %
X	0,03 %
Q	0,02 %

„Ist das nicht ganz schön viel Arbeit, wenn man einen Text auf diese Art knacken will?"

„Naja… es gibt leider Computerprogramme, die das für Mallory erledigen können. Das geht dann ruck-zuck, und er hat unseren Text entschlüsselt. Wir können uns am PC mal ein paar von diesen Werkzeugen ansehen."

Aufgabe:

Recherchiere im Internet und suche entsprechende Werkzeuge zur Häufigkeitsanalyse!

Die Vigenère-Chiffre

„Gibt es denn keine Möglichkeit, diese Häufigkeitsverteilung zu verschleiern?", wollte Alice wissen.

„Doch… ein gewisser Herr Vigenère hatte eine interessante Idee. Er dachte sich, dass man die Verschlüsselungstabelle bei jedem Buchstaben wechseln kann."

„Das verstehe ich nicht…"

„Zuerst machen wir ein Codewort aus, z.B. „Hundepfote". Und nun nehmen wir mal an, du willst „hallo bob lass uns ins kino gehen" verschlüsseln. Den Text schreibst Du auf und darunter das Wort „hundepfote"

```
Klartext:   hallo bob lass uns ins kino gehen
Codewort:   hunde pfo tehu nde pfo tehu ndepf
-------------------------------------------
Geheimtext: ouyos qtp eezm hqw xsg dmui thlts
```

Die Buchstaben werden einfach addiert. ‚h' + ‚h' ist zum Beispiel ‚o'!

„Häh??"

Aufgabe

Erklär Alice, wie das Addieren der Buchstaben funktioniert.

Alice war ganz begeistert: „Super, das ist doch genau das, was wir brauchen. Das erste „l" von „hallo" wird durch einen anderen Buchstaben als das zweite „l" ersetzt. Dafür hat das „h" und das zweite „l" den gleichen Buchstaben."

„Genau! Und genau das verhindert, dass Mallory mit Buchstaben zählen irgendetwas erreicht. Und es nützt ihm auch nichts, wenn er weiß (oder vermutet), dass „hallo bob" im Geheimtext „ouyos qtp" heißt. Damit kann er nicht viel anfangen.". Bob war sich sicher, nun das perfekte System gefunden zu haben!

Information:

Lange Zeit galt die Vigenère-Verschlüsselung tatsächlich als unknackbar, und wenn das Schlüsselwort „ziemlich lang" und der Klartext „ziemlich kurz" sind, dann ist es in der Tat schwer oder unmöglich, sie zu brechen. Hat man aber ein kurzes Schlüsselwort gewählt oder ist der Klartext im Vergleich zum Schlüssel lang, dann kann man den Geheimtext mit ziemlich raffinierten Tricks knacken. Auch wenn mehrere kurze Texte mit demselben Schlüsselwort verschlüsselt werden, hat der Angreifer ganz gute Möglichkeiten. Ohne Computerhilfe ist das Knacken aber in jedem Fall ziemlich aufwändig.

Die Hauptschwäche ist, dass das Codewort immer wiederholt wird, wodurch sich Muster ergeben, die raffinierte Codeknacker ausnutzen können.

Die sogenannte **Autokey-Chiffre** umgeht dieses Problem. Statt das Codewort zu wiederholen, setzt man einfach den Klartext selbst als Codewort ein.

```
Klartext:   hallo bob lass uns ins kino gehen
Codewort:   hunde pfo teha llo bob lass unsin
-------------------------------------------
Geheimtext: ouyos qtp eezs fyg jbt vifg arzma
```

Erst wenn ein Teil entschlüsselt ist, erhält man also die nächsten Buchstaben des Codewortes. Ziemlich pfiffig, aber pfiffige Codeknacker können auch diesen Code brechen. Leicht ist das nicht, aber die Kryptoanalyse, also die Wissenschaft vom Knacken von Codes, hat sehr große Fortschritte gemacht! Besonders dann, wenn der Angreifer einen

Teil des Klartextes kennt oder raten kann, dann lässt sich ohne größere Probleme zumindest einen Teil des Schlüssels ermitteln und damit oft auch den Rest der Nachricht entschlüsseln. Insofern hat Bob Unrecht wenn er sagt, dass Mallory nicht viel damit anfangen kann, wenn er weiß, dass "ouyos qtp" die Verschlüsselung von "hallo bob" ist.

Perfekte Sicherheit erreicht man übrigens, wenn das Schlüsselwort genauso lang wie der Klartext ist und aus zufälligen Buchstaben besteht. In diesem Fall kann man den Text (beweisbar) nicht knacken.

Allerdings ist der Preis für die perfekte Sicherheit hoch. Der Schlüssel ist sehr lang und er darf nur ein einziges Mal verwendet werden. Zudem muss man den Schlüssel auch geheim austauschen, so dass man dasselbe Problem wie bei der nun zu verschlüsselnden Nachricht hat. Allerdings kann man den Zeitpunkt für den Schlüsseltausch günstig wählen und ihn zum Beispiel während einer direkten Begegnung von Alice und Bob übergeben. Benutzen tut man ihn dann im ernsten Einsatz.

Tatsächlich kommt dieses als *One-Time-Pad* bezeichnete Verfahren zum Einsatz. In der Regel weicht man aber auf Verfahren mit deutlich kürzerem und wiederverwendbaren Schlüssel aus. Moderne Verfahren wie **Rijndael**, **Serpent** oder **Twofish** sind zwar nicht mathematisch beweisbar so sicher wie ein One-Time-Pad, praktische Untersuchungen haben aber bisher keine nutzbaren Schwächen aufgezeigt.

Exkurs: Vigenère in Java

Wenn du eine Programmiersprache beherrscht, dann lässt sich die Vigenère-Verschlüsselung recht leicht in einem Programm verwirklichen. Dies soll kurz am Beispiel der Sprache Java demonstriert werden.

```
// Das Programm kann nur Texte chiffrieren, die in Kleinbuchstaben
// geschrieben sind. Andere Zeichen werden einfach übernommen.
// Der Variablentyp char wird hier ebenso wie die Verwendung
// des ASCII aus didaktischen Gründen vermieden

String klartext = "hallo bob lass uns ins kino gehen";
String key = "hundepfote";
String geheimtext = "";
String alphabet="abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz";
int keypos = 0;

  for (int i = 0; i<klartext.length();i++){
    String eingabezeichen = klartext.substring(i,i+1);
    String ausgabezeichen = eingabezeichen;
    int stelle = alphabet.indexOf(eingabezeichen);
    if (stelle!=-1){
      int schieb = alphabet.indexOf(key.substring(keypos,keypos+1));
      ausgabezeichen = alphabet.substring(stelle+schieb,stelle+schieb+1);
      keypos++;
      if (keypos>=key.length()) keypos = 0;
    }
    geheimtext = geheimtext + ausgabezeichen;
   }
```

Aufgabe:

Erläutere das Programm und programmiere es nach. Bau Verbesserungen ein, so dass beispielsweise auch Großbuchstaben und Sonderzeichen erlaubt sind und geeignet chiffriert werden. Programmiere auch eine Entschlüsselungsmethode.

Transpositionschiffren - Der Würfel

Alice und Bob waren mit der Vigenère-Verschlüsselung sehr erfolgreich, denn das Knacken dieses Codes überstieg (vorerst) Mallorys Fähigkeiten. Aber er gab nicht auf. „Wenn ich schon ihren Code nicht brechen kann,", so dachte er sich, „denke ich mir eben auch einen Code aus und schreibe mir mit meiner Freundin Eve geheime Nachrichten – nur, um die beiden neugierig zu machen."

Er recherchierte ein wenig und fand ein System, das ihm gefiel. Er ging zu Eve und erklärte es ihr. „Also zuerst denken wir uns ein Codewort aus, vielleicht Katzenohr. Dann schreiben wir unsere geheime Nachricht in Spalten unter dieses Wort. Leerzeichen lassen wir weg, aber wir ergänzen ein paar zufällige Buchstaben, damit die Tabelle keine Löcher bekommt. Das ist zwar nicht unbedingt nötig, macht uns aber später das Entschlüsseln etwas einfacher. Allerdings nimmt dadurch auch die Sicherheit etwas ab!"

Er schrieb ein Beispiel auf:

HALLO EVE MEIN BRUDER WIRD SICH ÄRGERN

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

A B C D wurde ergänzt

„Dann sortieren wir das Codewort alphabetisch, so dass sich die Spalten verschieben."

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

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

„Und nun schreiben wir die Spalten einfach hintereinander. Zur besseren Lesbarkeit kann man z.B. Fünfergruppen bilden."

AIIGO RSNEE HCHEW REUIA VDCBM RÄDLN RELBB R

„Die Sache mit dem Vertauschen der Spalten kann man auch weglassen. Das Codewort brauchen wir dann nur noch, um die Spaltenzahl zu bestimmen. Das entspricht dann der sogenannten Skytale, darüber kannst du ja mal bei Wikipedia oder so nachlesen.

Die Variante ist zwar deutlich weniger sicher als mit Vertauschung, aber sie lässt sich einfacher mit dem Computer programmieren!", erklärte Mallory, der gerade dabei ist, Java zu lernen.

Information:

Eve ist neben Mallory häufig der Modellname für einen unbefugten Mithörer (engl. eavesdropper=Lauscher).

Eine Verschlüsselung, bei der die Position der Buchstaben vertauscht wird, heißt „Transpositionschiffre" (von lat. transponere = versetzen). Um eine solche Verschlüsselung zu brechen, ist schon ein gewisses Maß an Arbeit nötig, aber Profis (insbesondere solche mit einem Computer) knacken diesen Code ziemlich schnell.

Natürlich lässt sich diese Transposititon auch mehrfach hintereinander mit verschiedenen Codewörtern ausführen. Dadurch wird die Sicherheit drastisch erhöht.

Einfache Transposition

Mallory hat erwähnt, dass die Transpositionschiffre auch ohne Umsortieren der Spalten erfolgen kann. Dazu einigt man sich auf eine Spaltenzahl (z.B. 9) und trägt den Text ein. Leerzeichen kann man dabei weglassen:

```
HALLO EVE MEIN BRUDER WIRD SICH ÄRGERN

H A L L O E V E M
E I N B R U D E R
W I R D S I C H Ä
R G E R N A B C D       A B C D wurde ergänzt
```

Und nun schreibt man die Spalten einfach hintereinander:

```
HEWRAIIGLNRELBDRORSNEUIAVDCBEEHCMRÄD
```

Wenn man nun noch Fünfergruppen bildet, dann hat man eine übersichtlichere Version:

```
HEWRA IIGLN RELBD RORSN EUIAV DCBEE HCMRÄ D
```

Wie gesagt: Diese Variante ist im Vergleich zum echten Würfel sehr viel unsicherer; das sieht man schon daran, dass der Schlüssel nur aus einer Zahl besteht und es daher nicht viele Varianten gibt - im Zweifelsfall probiert man alle möglichen Tabellengrößen einfach durch.

Allerdings lässt sich dieses Verfahren recht einfach in einer Programmiersprache umsetzen, die Grundidee soll hier kurz erläutert werden:

```
String a = "HALLOEVEMEINBRUDERWIRDSICHÄRGERN";
String geheim = "";
for (int i=0;i<a.length();i=i+9){
 geheim = geheim + a.substring(i,i+1);
}
```

Die Grundidee besteht darin, dass man durch den String "durchhüpft". Die Buchstaben, die in der ersten Spalte stehen, haben Positionen im String, die Vielfache von 9 sind, da die Tabelle 9 Spalten hat. Auf diese Art kann man sich die Buchstaben der ersten Spalte herauspicken.
Die Buchstaben der zweiten Spalte bekommt man, indem man zu den Indices der ersten Spalte 1 addiert. Das grün markierte "E" oben hat beispielsweise den Index 9, das daneben stehende "I" den Index 10. Auf diese Weise konstruiert man nach und nach alle 9 Spalten und hängt die Buchstaben an den Ausgabestring `geheim` an. Mit geschickter Benutzung von Schleifen kann man die Zahl 9 auch variabel gestalten.

Die hier vorgestellte Transposition ist alleine recht schwach, kann aber eine vorhergehende oder nachfolgende Substitution gegebenenfalls verstärken.

Die Gartenzaunchiffre

Auch Eva hatte ein wenig recherchiert und schlägt Bob die Gartenzaunchiffre vor.

„Wir notieren unseren Text zick-zack-förmig in einer Tabelle und schreiben dann die Zeilen hintereinander."

„Hä?"

„Pass auf, ich zeige dir ein Beispiel!"

Klartext: HALLO BOB DAS IST EIN BEISPIEL

„Zuerst entfernen wir die Leerzeichen und tragen das Ganze dann in eine Tabelle ein."

H						O						S						E					L
	A				B		B				I		T				B		I				E	
		L		O				D		S				E		N				S		I		
			L						A						I						P			

„Und nun schreiben wir einfach die Zeilen hintereinander. Also zuerst H O S E L, danach A B B I T B I E und so weiter."

Geheimtext: HOSELABBITBIELODSENSILAIP

„Hm... das sieht ganz gut aus.", meinte Bob. „Und was ist dabei der Schlüssel?"

„Ganz einfach: Die Zahl der Zeilen ist natürlich nicht unbedingt 4, wir können da sehr flexibel sein. Außerdem könnten wir die Buchstaben natürlich auch in einer anderen Reihenfolge eintragen oder statt einer rechteckigen Tabelle vielleicht eine andere Form wählen. Wir könnten auch zur Verwirrung noch eine Buchstabenersetzung durchführen. Die Möglichkeiten sind da sehr vielfältig."

Aufgabe:

Entschlüssle die folgende Nachricht, die mit einer Tabelle mit 6 Zeilen verschlüsselt worden ist: STDUSENEPASANEHVTRUESDR

Zwischenprüfung

1. Erkläre, wie die Geheimschrift von Cäsar funktioniert.
2. Das Verfahren von Cäsar und das Verfahren von Vigenère gehören beide zu den so genannten _____.
3. Erkläre die Begriffe „brute force attack" und „known plaintext attack".
4. Erkläre, wie die Vigenère-Verschlüsselung funktioniert und welchen Vorteil sie gegenüber dem System von Cäsar besitzt.
5. Was besagt der Grundsatz von Kerckhoffs?
6. Jemand schlägt vor, einen Text mit dem Verfahren von Cäsar zu verschlüsseln und danach den Geheimtext ein zweites Mal mit dem Verfahren von Cäsar zu verschlüsseln. Beurteile, ob dadurch die Sicherheit erhöht wird.
7. Nun soll ein Text zweimal mit dem Verfahren von Vigenère verschlüsselt werden. Das erste Mal wird das Wort „Katze" verwendet, das zweite Mal das Wort „Hund". Wird dadurch die Sicherheit erhöht?
8. Welches Passwort ist für die Vigenère-Verschlüsselung besser: „Kerker" oder „Knast"? Begründe!
9. „Die Cäsar-Verschlüsselung ist ein Spezialfall der Vigenère-Verschlüsselung." Stimmt diese Behauptung?

Faires Spiel - Die Playfairchiffre

Mallory hat sich informiert und stellt Eve ein weiteres Verschlüsselungsverfahren vor.

„Bob und Alice haben bei ihren Verschlüsselungen immer nur einzelne Buchstaben ersetzt, also z.B. A durch X, B durch L usw. Man kann aber auch Paare ersetzen!", referierte er.

„Also zum Beispiel ER durch UZ und EN durch KL?", frage Eve nach und Bob nickte. Er hatte gelesen, dass eine solche Ersetzung viel schwieriger zu knacken ist, als wenn man nur einzelne Buchstaben betrachtet.

„Wow.... da gibt es aber viele Kombinationen....26 mal 26 .... macht 676 Paare.", rechnete Eve schnell nach.

„Ja.... und genau das macht die Sicherheit aus!", freute sich Bob.

„Aber.... 676 Kombinationen.... ich muss mir doch irgendwie notieren, welches Paar wodurch ersetzt wird. Das ist ein wenig Aufwand."

„Nicht wirklich! Es gibt da nämlich einen kleinen Trick. Wir denken uns wie immer ein Codewort aus und schreiben das Alphabet in eine 5x5-Tabelle. Zuerst das Codewort und dann die restlichen Buchstaben."

„5x5 ist 25, aber das Alphabet hat 26 Buchstaben....."

„Kein Problem.... das Y braucht man sowieso nie, das lassen wir einfach weg. Und wenn es doch mal auftaucht, dann schreiben wir halt ein i...."

Bob notierte ein Beispiel. Er wählte als Codewort „dampfschiff", wobei er die letzten beiden f weggelassen hatte, da das f bereits verbraucht war.

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

„Und jetzt?", wollte Eve wissen.

„Angenommen, wir wollen das Wort FISCHE verschlüsseln. In Paaren geschrieben ist das FI SC HE. Nun suchen wir die Buchstaben F und I im Quadrat und denken uns ein Rechteck bei diesen Buchstaben:

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

Wir ersetzen nun das Paar FI einfach durch die beiden Buchstaben an den anderen Ecken dieses Rechtecks, also PB oder BP.... da muss man sich vorher einigen. Bei Paaren in derselben Zeile oder Spalte wie bei SC nimmt man einfach jeweils den linken oder rechten Nachbarn. Aus SC machen wir also vielleicht CH, aus IB würde dann BS werden. Am Ende der Zeile oder Spalte geht es dann also einfach wieder von vorne los.

Information:

Wenn du an den genauen Ersetzungsregeln des „Original-Playfair" und an weiteren Details wie der Handhabung von Doppelbuchstaben interessiert bist, dann kannst du sie beispielsweise bei Wikipedia nachlesen.

Gar nicht so geheime Codes – Morsezeichen und andere

Codes werden nicht nur zum Geheimhalten von Informationen benutzt. Häufig muss man einfach Buchstaben durch andere Zeichen oder Symbole ersetzen, weil es nicht anders geht.

Bekannt ist zum Beispiel der Morse-Code, mit dessen Hilfe man Buchstaben (und auch andere Zeichen) nur mithilfe der Symbole „lang" und „kurz" darstellen kann. So kann man Buchstaben zum Beispiel mit einer Lampe, durch Klopfzeichen oder mit Pfiffen übertragen.

Sicher kennst Du das SOS-Signal für ein Schiff in Seenot. Durch die Folge „kurz kurz kurz lang lang lang kurz kurz kurz" oder einfach ··· - - - ··· übermittelt man die Buchstaben „S O S", was als „save our souls" (Rettet unsere Seelen) oder „save our ship" interpretiert werden kann. Der Buchstabe S wird also durch ··· ersetzt, der Buchstabe O durch - - -. Jeder Buchstabe hat eine solche Folge aus kurzen und langen Signalen, die man in einer Tabelle darstellen kann. Es handelt sich also um ein Substitutionsverfahren.

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	– – · ·

Ein Computer kann, tief im Inneren, nur mit zwei Zuständen, nämlich „Strom an" oder „Strom aus" etwas anfangen. Ein Prozessor ist (vereinfacht gesagt) nichts anderes als ein Sammlung vieler Schalter, die bestimmte Leitungen entweder an oder aus schalten können. Auch wenn wir auf unserem Bildschirm den Buchstaben „A" sehen, so ist das Ganze für den PC im Inneren nur eine gewisse Schalteranordnung. Ähnlich wie im Morsecode kann nun jedes Zeichen durch eine Folge von „1" (Strom an) und „0" (Strom aus) dargestellt werden. Eine solche „1" oder „0" heißt in der Computersprache „bit".

Aufgabe:

Erinnere Dich an das Dualsystem (Mathe, Klasse 5) und erkläre, wie es funktioniert.

Informiere Dich über den so genannten „ASCII" und seine Erweiterungen.

Begriffe zur Kryptologie

Kryptologie	Das ist die Wissenschaft der Geheimschriften. Häufig wird der Begriff "Kryptographie" gleichbedeutend gebraucht, aber genaugenommen ist das nur die Lehre vom Verschlüsseln.
Klartext	Das ist der Text vor der Verschlüsselung, den jeder lesen kann, beispielsweise "HALLO BOB".
Geheimtext	Das ist der Text nach der Verschlüsselung, den man nicht mehr so ohne weiteres lesen kann, beispielsweise "REJVS ZYF".
Schlüssel	Das ist die geheime Information, die man braucht, um aus dem Geheimtext wieder den Klartext zu machen, z.B. ein Codewort.
Verschlüsseln Codieren	Man überführt den Klartext mithilfe des Schlüssels in den Geheimtext.
Entschlüsseln Decodieren	Man überführt den Geheimtext mithilfe des Schlüssels in den Klartext.
Brechen/Knacken einer Verschlüsselung	Man macht aus dem Geheimtext den Klartext, ohne dass man den Schlüssel kennt, oder man ermittelt den Schlüssel irgendwie aus dem Geheimtext.
Substitutions-verschlüsselung	Die Buchstaben des Klartextes werden durch andere Buchstaben oder durch Zeichen ersetzt. Beispiele: Cäsar, Vigenère, ROT 13, Playfair
monoalphabetische Substitution	Jedes Klartextzeichen wird stets zum selben Geheimtextzeichen, also z.B. jedes "A" im Klartext ist ein "D" im Geheimtext usw. Beispiel: Cäsar-Verschlüselung
polyalphabetische Substitution	Jedes Klartextzeichen hat verschiedene Geheimtextzeichen. Das erste "A" wird beispielsweise ein "Q", das zweite "A" ein "X", das dritte "A" ein "V" usw. Beispiel: Vigenère-Verschlüsselung
Transpositions-verschlüsselung	Die Buchstaben des Klartextes werden nach einem gewissen Schema durcheinandergewürfelt, dabei aber nicht verändert. Ein "A" bleibt also ein "A", aber es kommt an eine andere Stelle. Beispiele: Gartenzaun, Skytale
Überschlüsselung	Ein Klartext wird verschlüsselt und dann wird der so erhaltene Ge-heimtext nochmal (ggfs. mit einem anderen Verfahren) verschlüsselt. Das KANN die Sicherheit verbessern und das Knacken erschweren, aber in vielen Fällen tut es das nicht (wesentlich).