Lesetext Kryptographie

L201

Aufgabe:

Lies den folgenden Text einmal für dich durch. Markiere Stellen, die dir wichtig erscheinen.

Beantworte die Fragen am Ende des Textes möglichst genau.

Zeit: 45‘ **Sozialform:** EA

„Treffen morgen um fünf hinter der Schule.” Stell dir vor, du willst dich mit einer Freundin verabreden, aber leider möchte ihr großer Bruder das verhindern. Wenn er mitbekommt, dass ihr euch verabredet habt, wird er störend dazwischenfunken. Deshalb musst du deiner Freundin die Nachricht heimlich zukommen lassen oder so verändern, dass ihr Bruder sie nicht lesen kann. Das Beispiel mag aus der Luft gegriffen scheinen. Aber tagtäglich tauschen Menschen Nachrichten per Funk, per Telefon, per E-Mail oder Post miteinander aus, und immer wieder gibt es andere, die wollen mitkriegen, was da gesagt, geschrieben oder übermittelt wird. Gegen diese ungebetenen Lauscher gibt es Tricks: Geheimschriften und versteckte Mitteilungen.

WARUM NACHRICHTEN GEHEIM VERSENDEN

Gerade heutzutage werden viele wichtige Informationen übermittelt, die niemand unerlaubt mitlesen sollte. So kaufen viele Leute über das Internet ein oder überweisen Geld mit dem Computer (Onlinebanking). Nicht auszudenken, wenn jemand anderes die Konto- oder Kreditkartennummern mitlesen könnte – plötzlich hebt jemand einfach Geld vom Bankkonto eines anderen ab!

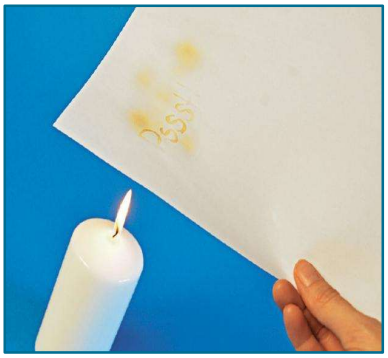
Daher versteckt man entweder Nachrichten, die geheim bleiben sollen, oder man verändert sie so, dass nur der Absender und der Empfänger sie lesen können.

Caesar nutzte eine Geheimschrift
Der römische Feldherr Julius Caesar übermittelte seine Kriegspläne in einer Geheimschrift, denn er wollte verhindern, dass seine Gegner seine nächsten Schritte herausfinden.

MIT GEHEIMTINTE UND CO. - NACHRICHTEN VERSTECKEN

Du schreibst einen scheinbar harmlosen Brief an deine Freundin: „Liebe Lena, für morgen müssen wir in Mathe die Aufgabe 5a bis d auf Seite 8 lösen.”

Lenas großer Bruder erhascht einen Blick auf den Brief, ohne etwas Verdächtiges feststellen zu können. Was er nicht weiß: Du hast auf das Papier noch etwas mit einer unsichtbaren Tinte geschrieben – mit Geheimtinte. Dazu hast du eine halbe Zitrone ausgepresst, einen dünnen Pinsel in den Zitronensaft getaucht und deine Nachricht geschrieben: „Treffen morgen …” Du musstest sie blind schreiben, denn der Zitronensaft ist durchsichtig. Nachher weiß Lena, was sie zu tun hat: Sie erwärmt den Brief vorsichtig über einer brennenden Kerze. Deine Nachricht wird unter dem unverfänglichen Text als bräunliche Schrift sichtbar. Du hättest die Nachricht übrigens auch mit Milch oder Essig schreiben können.



Verstecken durch Prägen
Du kannst eine Nachricht auch mittels Prägung verstecken. Dazu legst du auf deinen Brief mit dem unverfänglichen, harmlosen Text ein zweites Blatt Papier. Mit einem Bleistift oder Kugelschreiber schreibst du die Nachricht auf das obere Blatt, wobei du so fest aufdrückst, dass sich die Nachricht in den darunter liegenden Brief eindrückt. Dann wirfst du das obere Blatt weg. Die geheime Nachricht ist auf dem Brief kaum zu erkennen. Wenn der Empfänger den Brief mit schräg gestelltem Bleistift schraffiert, wird die versteckte Nachricht als weißer Text sichtbar.

NACHRICHTEN VERSCHLÜSSELN

Heute werden Nachrichten nicht mehr versteckt an den Empfänger geschickt – schließlich kann man den ganzen Funk- Telefon-, Post- oder E-Mail-Verkehr nicht heimlich abwickeln. Stattdessen werden vertrauliche Nachrichten so verändert, dass nur der sie lesen kann, für den die Nachricht bestimmt ist. Das nennt man verschlüsseln. Der Empfänger kennt das Verfahren, mit dem die Nachricht verschlüsselt wurde, und kann sie wieder entschlüsseln.

Lena hat eine verschlüsselte Nachricht an dich verfasst. Sie lautet „adfnüfmunegromnib". Kannst du sie entziffern? Man kann eine Nachricht ganz einfach verändern, indem man die Buchstaben vertauscht: Aus dem Wort „und" wird dann z. B. nud, dnu oder ndu. Solch eine Verschlüsselung ist aber recht leicht zu knacken – Lenas Nachricht muss man einfach nur rückwärts lesen.

Eine der ältesten bekannten Verschlüsselungen ist eine Transposition. Die Regierung von Sparta benutzte vor über 2500 Jahren zur Verschlüsselung eine sogenannte Skytale. Die Buchstaben bleiben was sie sind, aber nicht wo sie sind. Solche Verschlüsselungen heißen Transposition. (Das Wort Transposition ist abgeleitet vom lateinischen Wort transponere = verschieben.)

Verschlüsselung im alten Sparta
Vor rund 2 500 Jahren verschlüsselten die Spartaner in Griechenland ihre Nachrichten, indem sie die Reihenfolge der Buchstaben veränderten. Dazu nutzten sie ein ausgefeiltes Verfahren: Sie nahmen ein schmales Pergamentband und wickelten es um einen Holzstab, so wie man einen Verband um einen Arm wickelt. Dann schrieben sie den Text normal von links nach rechts quer über die ganze Länge des Stabes auf das aufgewickelte Band, Zeile für Zeile.
Wenn das Band abgewickelt wurde, standen darauf irgendwelche Buchstaben untereinander, die scheinbar keinen Sinn ergaben.
Wie setzte man die Nachricht wieder zusammen? Der Empfänger hatte einen Stab gleicher Dicke. Er wickelte das Pergamentband um seinen Stab, und die Nachricht wurde lesbar. Den Holzstab und im übertragenen Sinn auch die verschlüsselte Nachricht nannten die Spartaner Skytale.

DAS CAESAR-VERFAHREN: BUCHSTABEN DURCH ANDERE ERSETZEN

Bei den heutigen Verschlüsselungsverfahren werden die Buchstaben in der Nachricht durch andere Buchstaben oder auch durch ganz andere Zeichen ersetzt (also auch Ziffern oder Sonderzeichen). Solch eine Methode, bei der Buchstaben durch andere Buchstaben ersetzt werden, hat schon Julius Caesar verwendet. Und auch Lena kennt dieses Caesar-Verfahren:

Sie hat wieder eine Mitteilung verfasst. Ihr Bruder konnte sogar einen Blick darauf erhaschen und sie abschreiben, aber was da steht, kann er nicht lesen: odvv xqv xqv vfkrq khxwh xp ixhqi wuhiihq. Du kannst es entschlüsseln, weil du weisst, wie Lena vorgegangen ist: Lena hat jeden Buchstaben durch einen anderen Buchstaben ersetzt, und zwar einfach um den Buchstaben, der drei Stellen weiter hinten im Alphabet steht, also D statt A, E statt B usw.

Um nicht bei jedem Buchstaben wieder von neuem abzählen zu müssen, hat Lena eine Tabelle angefertigt: Oben stehen in einer Zeile die Buchstaben des Klartextalphabets, also das normale Alphabet; darunter stehen die entsprechenden Buchstaben aus dem Geheimtextalphabet. Da es keinen Buchstaben gibt, der drei Stellen hinter dem X steht, hat Lena wieder von vorne begonnen

und statt dem X ein A eingesetzt. Um das Wort „fünf” zu verschlüsseln, hat sie es erst mal als „fuenf” geschrieben. Die Umlaute Ä, Ü und Ö werden also zu AE, UE und OE, und aus einem ß wird SS.

Zum Entschlüsseln suchst du für jeden Buchstaben des Geheimtextalphabets den passenden normalen Buchstaben aus dem Klartextalphabet. Wie lautet die richtige Nachricht? Zur Kontrolle steht die Lösung hier noch einmal rückwärts: neffert fnüf mu etueh nohcs snu snu ssal.

Caesar-Verfahren
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
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

Die Buchstaben bleiben wo sie sind, aber nicht was sie sind. Solche Verschlüsselungen heißen Substitution. (Das Wort Substitution ist abgeleitet vom lateinischen Wort substituere = ersetzen.)

KRYPTOGRAPHIE

Verfahren, die sich mit dem Ver- und Entschlüsseln von Nachrichten befassen, nennt man Kryptographie. Das Wort kommt aus dem Griechischen, und zwar von den Wörtern *kryptein* für „verbergen” und *graphein* für „schreiben”. Um sich mittels Geheimnachrichten verständigen zu können, einigen sich der, der die Nachricht losschickt, und der, der die Nachricht empfängt, auf einen Schlüssel, mit dem die Nachricht ver- und entschlüsselt werden kann. Das ist so, als würde Lena ihre Nachricht vor dem Verschicken mit ihrem Schlüssel in einem Safe einschließen. Du erhältst diesen Safe, öffnest ihn mit deinem Schlüssel und kannst die Nachricht lesen.

Seit es verschlüsselte Nachrichten gibt, gibt es auch Leute, die diese Nachrichten zu entziffern versuchen, obwohl gerade sie diese Nachrichten nicht lesen sollten. Mit viel Zeit gelingt es häufig, auch verschlüsselte Nachrichten zu entziffern. Das Verfahren, das Caesar benutzt hat, wäre heute jedoch leicht zu knacken. Deshalb hat man immer bessere Verschlüsselungsverfahren entwickelt. Bei den neusten Verfahren müssten Computer unendlich lange rechnen, um eine Nachricht zu entziffern.

CODES KNACKEN

Wie kann man ohne Schlüssel eine durch Substitution verschlüsselte Nachrichten entziffern? Über eine Häufigkeitsanalyse. Jeder Code, bei dem Buchstaben durch Symbole oder andere Buchstaben vertauscht werden, hat eine entscheidende Schwachstelle. Man schaut nach, welches das häufigste Zeichen ist. Das könnte das »E« sein. Ebenso verfährt man mit dem zweithäufigsten Zeichen, und so weiter. Du brauchst dazu eine Tabelle, wie häufig jeder Buchstabe in einer bestimmten Sprache vorkommt. Ein Ausprobieren aller Kombinationen wäre viel zu aufwändig. In jeder Sprache kommen einige Buchstaben häufiger vor als andere. Diesen Umstand kann sich ein Code-Knacker zu Nutze machen.

In der Deutschen Sprache kommt der Buchstabe „E“ am häufigsten vor, gefolgt von den Buchstaben „R“, „N“, „S“, „T“ und „L“. Dies kannst du dir leicht mit dem Namen „ERNST“ merken.

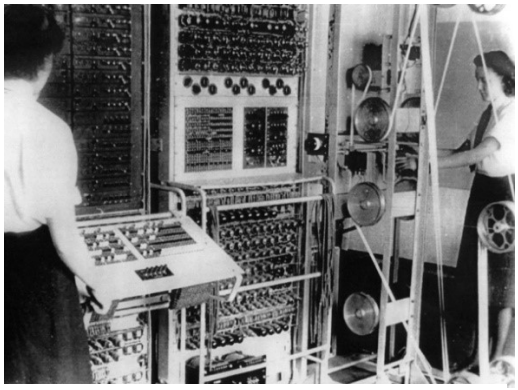
Alles was du jetzt zu tun brauchst, ist Buchstaben oder Symbole zählen. Das Zeichen, das am häufigsten vorkommt, ist mit grosser Wahrscheinlichkeit der Buchstabe „E“. Stelle das Cäsar‘s Rad so ein, dass der gezählte Buchstabe mit „E“ übereinstimmt und probiere, die ersten Wörter zu entschlüsseln. Wenn diese keinen Sinn ergeben, stellst du das Rad auf „R“ ein und versuchst es erneut. Fahre nach diesem Muster weiter, bis du den Code geknackt hast.

ENIGMA – SPIONAGE UND GEGENSPIONAGE

Im 2. Weltkrieg versandte das deutsche Militär viele Nachrichten über Funk. Die Kriegsgegner, die Alliierten, hörten den Funk ab, konnten aber zuerst nichts damit anfangen, denn die Nachrichten waren verschlüsselt. Dazu verwendeten die Deutschen eine Maschine, die sie Enigma nannten. Das ist Griechisch und heißt Rätsel. Wie du hier sehen kannst, hatte Enigma Ähnlichkeit mit einer Schreibmaschine.

Die Empfänger der so verschlüsselten Nachrichten konnten dann mit einer zweiten Enigma-Maschine die Funksprüche entschlüsseln. Das Prinzip der Enigma ist sehr kompliziert. Buchstaben werden mit Hilfe von Walzen verschlüsselt. Je mehr Walzen die Maschine hat, desto komplizierter ist es, den Code zu knacken.

Zusätzlich können die Einstellungen der Walzen verändert werden. Das macht das Entschlüsseln noch schwieriger. Die codierte Nachricht kann nur von einer Enigma mit denselben Einstellungen gelesen werden. Wenn man einen Buchstaben tippte, wies die Maschine ihm einen anderen Buchstaben zu – und das nach einem komplizierten, sich ständig ändernden Verschlüsselungssystem, das rund 150 Billionen verschiedene Möglichkeiten zuließ.



Aufnahme der "Colossus", die in England während des Zweiten Weltkriegs ab 1943 gebaut wurde, um die Botschaften der Enigma zu entschlüsseln.

Gleichzeitig arbeiteten Engländer, Franzosen und Amerikaner daran, den Code zu knacken. Spezialisten beschäftigten sich rund um die Uhr mit der Entschlüsselung der deutschen Funksprüche, bis es ihnen 1941 zum ersten Mal gelang. Da die Einstellungen der Maschinen aber ständig verändert wurden, musste auch weiterhin für jeden Funkspruch der passende Code gefunden werden. Das dauerte so lange, dass die geknackten Funksprüche jedes Mal veraltet waren. Irgendwann fielen den Alliierten einige der Maschinen in die Hände, sie fanden den Schlüssel heraus und konnten die deutschen Funksprüche entziffern. Dadurch waren sie über einige Pläne des deutschen Militärs im Bilde und konnten die Dauer des Krieges abkürzen.

Um den Code schneller zu knacken, entwickelte der Mathematiker Alan Turing eine Rechenmaschine in Schrankgröße - die sogenannte "Turing-Bombe". Damit konnten die Enigma-Nachrichten ab 1943 entschlüsselt werden. Enigma wurde übrigens weiterentwickelt und bis in die achtziger Jahre des 20. Jahrhunderts von verschiedenen Geheimdiensten genutzt.

VERSCHLÜSSELN HEUTE

Mit Internet und Co. nimmt die Bedeutung der Verschlüsselung zu. Jede E-Mail, die du versendest, kann von einem Unbefugten gelesen werden. Denn auf dem Weg zum Empfänger passiert sie viele Rechner, wo sie abgefangen werden kann. Man sagt auch, eine E-Mail ist offen wie eine Postkarte. Damit doch nicht jeder Beliebige deine E-Mails lesen kann, gibt es spezielle Programme, mit denen sich E-Mails verschlüsseln lassen. Beim Onlinebanking oder beim Einkaufen über das Internet gibt es ebenfalls spezielle Verschlüsselungsverfahren. Man erkennt sie z. B. daran, dass in der Internetadresse nicht http://www…, sondern https://www… steht. Das „s" vor dem Doppelpunkt in der Adresse signalisiert, dass der Datenverkehr zwischen dir und dem Empfänger sicher sein soll.

Fragen zum Textverständnis

1. Das Wort „Kryptografie“ stammt aus der lateinischen Sprache und bedeutet „Kringelige Schrift“.
   - ☐ richtig
   - ☐ falsch, richtig ist: .....

2. Heute werden in E-Mails digitale Geheimtinten genutzt, um Nachrichten vor Unbefugten zu verstecken.
   - ☐ richtig
   - ☐ falsch, richtig ist: .....

3. Man kann eine Nachricht verschlüsseln, indem man die Buchstaben oder deren Reihenfolge vertauscht.
   - ☐ richtig
   - ☐ falsch, richtig ist: .....

4. Mit der Verschlüsselungsmethode „Substitution“ wird die Reihenfolge der Buchstaben geändert..
   - ☐ richtig
   - ☐ falsch, richtig ist: .....

5. Verbinde die Satzteile in der Tabelle miteinander.

1.	Bei den neusten Verschlüsselungsverfahren müssten Computer unendlich lange rechnen,	a.	nennt man solche Verschlüsselungen *Substitution*.
2.	Wenn die Buchstaben bleiben was sie sind, aber nicht wo sie sind,	b.	entwickelte der Mathematiker Alan Turing eine Rechenmaschine.
3.	Damit doch nicht jeder Beliebige deine E-Mails lesen kann,	c.	eine Nachricht für den unbefugten Leser unverständlich zu machen.
4.	Geheimtinten dienen dazu,	d.	um Bankdaten und andere vertrauliche Informationen sicher zu machen.
5.	Verfahren, die sich mit dem Ver- und Entschlüsseln von Nachrichten befassen,	e.	nennt man solche Verschlüsselungen *Transposition*.
6.	Wenn die Buchstaben bleiben wo sie sind, aber nicht was sie sind,	f.	um eine geschützte Nachricht zu entziffern.
7.	Chiffrierte Nachrichten dienen dazu,	g.	kannst du deine E-Mails mit speziellen Programmen verschlüsseln.
8.	Verschlüsselte Daten im digitalen Datenverkehr dienen dazu,	h.	um eine Nachricht vor einem unbefugten Leser zu verstecken.
9.	Um den Code schneller zu knacken,	i.	nennt man Kryptographie.