Vorwort

Schon viele tausend Jahre lang werden Nachrichten verschlüsselt, um geheime Botschaften auszutauschen und Informationen sicher vor dem Einblick anderer zu schützen. Im heutigen Internetzeitalter ist die Verschlüsselung aus dem Alltag nicht mehr wegzudenken.

Der Fachbegriff für die Verschlüsselung lautet, **Kryptografie.** Das Wort setzt sich aus den altgriechischen Wörtern kryptós, auf Deutsch ‚verborgen', ‚geheim' und gráphein, auf Deutsch ‚schreiben' zusammen. Kryptografie lässt sich also mit geheim schreiben übersetzen.

Darum geht es auch: einen Klartext, den jeder lesen kann, so zu verändern, dass ihn nur der wieder entschlüsseln kann, der den geheimen Schlüssel kennt.

In diesem Studienbrief lernst du verschiedene Verschlüsselungsverfahren kennen und entwickelst selbst Verschlüsselungen. Du erfährst etwas über die Geschichte der Verschlüsselung und lernst, wie man Geheimtinten herstellt.

Neben diesem Text gibt es im Modul Lernvideos, Quize und ein Rätsel, dass es zu lösen gibt.

Lernziele:

Wenn du das Modul bearbeitet hast …

… kannst du symmetrische und asymmetrische Verschlüsselung unterscheiden.

… kannst Sätze und Wörter mit verschiedenen Methoden Ver- und Entschlüsseln.

… kannst erklären, was ein Algorithmus ist.

… kennst die Bedeutung der Verschlüsselungsmaschine „Enigma"

.. kennst die Einsatzgebiete von Verschlüsselungen

… kannst erklären wozu ein „Hashwert" dient.

… kannst selbst Geheimtinte herstellen, verwenden und sichtbar machen.

Kontakt

Bei Fragen zum Modul und den Inhalten kannst du gerne eine E-Mail an

Birger-Daniel Grein (info@grein-media.de) wenden!

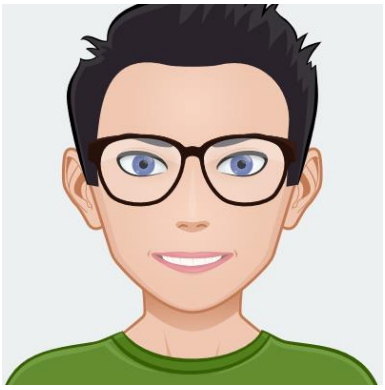
Aufgabentypen

Im Studienbrief gibt es zwei Aufgabentypen.

Bei **Fragen** sollst du selbst Lösungen überlegen und eigene Ideen finden.

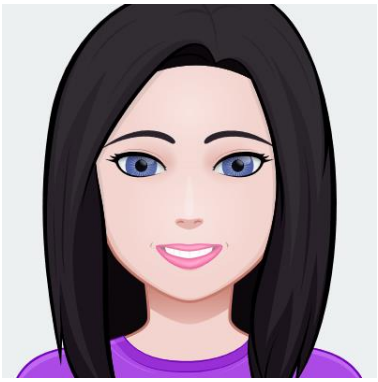
Mit **Übungen** testest du dein Verständnis für eine Erklärung. Die Lösung für Übungen findest du am Ende des Studienbriefs.

Die Geheime Nachricht



Die Geschwister Henrik und Lena lieben Geheimnisse. Deshalb haben sie natürlich auch ein Geheimversteck. An einem Samstag wollen sie ihre neue Freundin Amelie das erste Mal dorthin einladen. Doch sie wollen sicher gehen, dass niemand Fremdes das Versteck findet.

Deshalb senden sie Amelie folgende Nachricht.



Liebe Amelie,

wir freuen uns, dass wir der das erste Mal unser Geheimversteck zeigen können. Du findest es einmal beim:

ipmatdivqqfo

Amelie schaut den Brief fragend an. Wo soll, dass Versteck denn sein? Da fällt ihr auf, dass das Wort einmal unterstrichen ist und das Bild auf dem Brief, der römische Herrscher Julius Caesar zu sehen ist.

Sie ist sich sicher, dass muss der Schlüssel sein.

Frage: Hast du eine Idee, wo sich das Versteck befindet?

Die Caesar-Chiffre

Unter einer Chiffre versteht man eine Geheimschrift. Die Cäsar-Chiffre ist nach dem römischen Staatsmann Gaius Julius Cäsar benannt. Er lebte 100 vor Christus bis 44 vor Christus in Rom. Er soll die Verschlüsselung benutzt haben, um Nachrichten während seiner Kriege zu versenden, ohne dass die Gegner mitlesen konnten.

Die Caesar-Chiffre funktioniert durch Verschiebung der Buchstaben, um eine bestimmte Anzahl im Alphabet. Dabei ist es egal, ob es sich um Großbuchstaben oder Kleinbuchstaben handelt. Ob, du die Wörter alle klein schreibst, oder so wie es in der Rechtschreibung richtig ist, bleibt dir überlassen.

Amelie überlegt sich: Wenn Henrik und Lena die eins unterstreichen, heißt das bestimmt, ich muss jeden Buchstaben um eins verschieben.

Sie schreibt sich dazu eine Tabelle auf und denkt:

Nr.	1	2	3	4	5	6	7	8	9
Buchstabe	A	B	C	D	E	F	G	H	I

Nr.	10	11	12	13	14	15	16	17	18
Buchstabe	J	K	L	M	N	O	P	Q	R

Nr.	19	20	21	22	23	24	25	26	1
Buchstabe	S	T	U	V	W	X	Y	Z	A

Verschlüsselt man das A mit 1 muss ich einen Buchstaben weiter gehen:

Aus A wird B, aus B wird C und so weiter

Will ich das Z verschlüsseln beginne ich einfach wieder von vorne, also wird aus Z ein A.

Amelie überlegt weiter:

Wenn ich die Nachricht meiner Freunde entschlüsseln will, muss ich jeweils einen Buchstaben zurück gehen. Also wird aus einem B ein A und so weiter.

Frage: Wo befindet sich das Versteck der Geschwister! Nutze die Tabelle als Hilfe!

Lösung:

Aus dem i wird ein h, aus dem p wird ein o ….

Damit lautet der Ort des Geheimversteck: holzschuppen.

Merke: Derjenige der die Nachricht verschlüsselt, kann entschieden, um wie viele Buchstaben ein Buchstabe der Nachricht verschoben wird. Er muss dem Empfänger dann die verschlüsselte Nachricht, die Verschiebung und die Art der Verschlüsselung (hier das Caesar-Chiffre) mitteilen.

Übung:

A) Folgende Wörter wurden mit dem Caesar-Chiffre und der Verschiebung 3 verschlüsselt. Wie heißen sie unverschlüsselt (man sagt im Klartext)?

jduwhq

jhkhlpqlv

vfkrnrodghqhlv

B) Verschlüssle folgenden Satz selbst mit der Caesar-Chiffre und der Verschiebung 2! Tipp: Satzzeichen werden nicht verändert.

„hallo mein name ist amelie.“

Wie sicher ist die Caesar-Chiffre?

Die Caesar-Chiffre gilt als leicht zu knacken, da man nur ausprobieren muss, welche Verschiebung sinnvoll ist. Man kann sie etwas sicherer machen, indem man die verschlüsselte Nachricht, nochmal mit der Caesar-Chiffre und einer anderen Verschiebung verschlüsselt.

Beispiel:

Klartext	1. Verschlüsselung um 2 verschoben	2. Verschlüsselung um 1 verschoben
haus	jcwu	Kdxv

Vorgehen zum Entschlüsseln:

1. Verschiebe die Buchstaben um 1!

2. Verschiebe die Buchstaben aus dem Ergebnis um 2!

Merke: Um Nachrichten zu verschlüsseln und wieder zu entschlüsseln, braucht man genaue Handlungsanweisungen wie man vorgehen kann. Man nennt solche Anweisungen Algorithmen.

Sie sind auch in anderen Bereichen wichtig.
Schau dir dazu die Lernvideos an!

Verbesserungsideen für die Caesar-Chiffre

Um es Schlüsselknackern schwerer zu machen, kannst du zum Beispiel jeden Buchstaben eines Wortes mit einer anderen Verschiebung verschlüsseln.

Beispiel: Wir verschlüsseln das Wort „haus“:

Den ersten Buchstaben des Worts verschieben wir um 1!

Den zweiten Buchstaben des Worts verschieben wir ums 2!

Den dritten Buchstaben des Worts um 3!

und so weiter

Damit ergibt sich: H wird zu I, A wird zu C, U wird zu X und S wird zu W. Daraus folgt: „icxs“ als verschlüsselte Nachricht.

Aufgabe: Überlege dir weitere Möglichkeiten, die Caesar-Chiffre sicherer zu machen und probiere sie aus!

Weitere Chiffre die auf Verschieben von Buchstaben im Alphabet basieren

Verschlüsselung auf Basis eines Zahlenschlüssels

Die folgende Verschlüsselung funktioniert, wie die Verschiebung in der Caesar-Chiffre. Allerdings gibt jetzt der Zahlenschlüssel an, um wie viel ein Buchstabe verschoben wird. Du willst Lena und Henrik eine verschlüsselte Nachricht senden. Ihr habt als Zahlencode 2534 vereinbart. Du willst den kurzen Satz: „Ich bin da“ verschlüsseln.

Es gilt der Algorithmus:

Verschiebe das i um 2, es entsteht ein k

Verschiebe das c und 5, es entsteht ein h

Verschiebe das h um 3, es entsteht ein k

Verschiebe das b um 4, es entsteht ein f

Nun beginnt man wieder von vorne mit dem Code!

Verschiebe das i um 2, es entsteht ein k

Verschiebe das n um 5, es entsteht ein s

Verschiebe das d um 3, es entsteht ein g

Verschiebe das a um 4, es entsteht ein e

Die verschlüsselte Nachricht lautet: „khk fks ge“

Um die Nachricht wieder zu entschlüsseln musst du die Ziffer aus dem Code zurückgehen!

Übung:

A) Verschlüssle das Wort „blau“ mit dem Code 213!

B) Entschlüssle folgenden Geheimnachricht mit dem Code: 134!

„nrre“

C) „mama“ wurde zu “pbtd“. Wie lautet der dreistellige Verschlüsselungscode

Verschlüsseln mit einem Codewort oder Schlüsselsatz

Statt eine Zahl kann auch ein Wort oder Satz als Schlüssel dienen, um aus dem Klartext den Geheimtext zu erzeugen.

Der Vater der Geschwister hat Geburtstag. Lena möchte ihrem Bruder mitteilen, wo sie das Geschenk versteckt hat. Sie legt ihm dazu einen Zettel hin, da sie die Tage vor dem Geburtstag auf Klassenfahrt ist. Sie will ihm mitteilen:

„Das Geschenk ist im Schrank“

Damit kein anderer den Satz lesen kann, verschlüsselt sie ihn mit dem Namen ihres Kanarienvogels als Schlüsselwort. Der Vogel heißt „Hansi“.

Wie kann man den Satz mit dem Schlüsselwort Hansi verschlüsseln?

Der Satz zum Versteck soll durch Verschiebung der einzelnen Buchstaben im Alphabet erfolgen (wie bei der Caesar Chiffre).

Lena geht beim Verschlüsseln folgendermaßen vor:

1. Sie wandelt das Codewort in eine Zahl um! Dazu ordnet sie jedem Buchstaben zu, an welcher Stelle er im Alphabet steht.

Buchstabe	H	A	N	S	I
Stelle im Alphabet	8	1	14	19	9

2. Sie verschiebt jeden Buchstaben des Klartexts, um die Stelle im Alphabet, die das Codewort vorgibt.

Das D wird um 8 Stellen im Alphabet verschoben und wird zum L.

Das A wird um 1 Stelle im Alphabet verschoben und wird zum B.

Das S im Alphabet um 14 Stellen verschoben (nach dem Z wird wieder mit A begonnen) und wird zum G.

So geht es weiter. Leerzeichen werden einfach übernommen.

3. Wurde das Codewort einmal komplett verwendet, beginnt man beim nächsten Buchstaben des Klartexts wieder mit dem ersten Wert, d.h. dem H und verschiebt den Buchstaben um 8 Buchstaben im Alphabet nach vorne.

Übung: Wandle den Satz zum Versteck mit Hilfe des Codeworts „Hansi“ in eine Geheimnachricht um! Wie lautet sie?

Zum Entschlüsseln musst du die Verschiebung, die das Codewort erzeugt hat, einfach Rückgängig machen! Dazu gehst du von der Verschiebung des Geheimtexts mit Anzahl der Buchstaben zurück! Um zum Beispiel das L aus dem Geheimtext zu entschlüsseln, gehst du 8 Stellen im Alphabet zurück und landest beim D.

Alphabetische Verschlüsselung durch das Austauschen von Buchstaben

Wörter lassen sich auch dadurch verschlüsseln, dass man jedem Buchstaben einen anderen Buchstaben zuordnet. Der Partner muss dann die Entschlüsselungstabelle kennen.

Henrik und Lena verwenden folgende Liste:

Klartext	A	B	C	D	E	F	G	H	I
Verschlüsselt	Z	T	B	N	U	L	F	S	Q

Klartext	J	K	L	M	N	O	P	Q	R
Verschlüsselt	A	C	E	H	K	I	D	J	G

Klartext	S	T	U	V	W	X	Y	Z
Verschlüsselt	O	R	P	W	X	M	V	Y

So wird aus dem Wort lena: eukz

Übungen:

A) Verschlüssle folgendes Wort mit Hilfe der Tabelle von Henrik und Lena:

buch

B) Entschlüssle folgendes Wort mit der Tabelle der Geschwister:

zpri

Aufgabe:

Entwirf selbst eine Verschlüsselungstabelle und verschlüssle damit eine Nachricht! Lasse sie jemand aus deiner Familie entschlüsseln!

Austauschen von Buchstaben auf Basis eines Schlüsselworts

Um festzulegen, welcher Buchstabe durch welchen anderen Buchstaben ersetzt wird, kann man auch ein Schlüsselwort nutzen. Dann müssen Henrik und Lena nur das Schlüsselwort und nicht die ganze Tabelle zum Entschlüsseln weitergeben.

Dieses Schlüsselwort schreibt man unter ein normales Alphabet. Anschließend wird die untere Zeile mit den noch nicht benutzten Buchstaben in alphabetischer Reihenfolge aufgefüllt. Man beginnt dabei mit dem letzten verwendeten Buchstaben des Schlüsselworts. Wichtig kein Buchstabe darf doppelt vorkommen. Ein Buchstabe, der bereits in der zweiten Zeile steht, wird einfach übersprungen.

Beispiel:

Henrik und Lena haben Amelie das Schlüsselwort Geheimschrift mitgeteilt.

Zur Verschlüsselung ihrer Nachricht erstellen sie folgen Tabelle:

Buchstaben im Klartext	A	B	C	D	E	F	G	H	I
Buchstaben nach der Verschlüsselung	G	E	H	I	M	S	C	R	F

Buchstaben im Klartext	J	K	L	M	N	O	P	Q	R
Buchstaben nach der Verschlüsselung	T	U	V	W	X	Y	Z	A	B

Buchstaben im Klartext	S	T	U	V	W	X	Y	Z
Buchstaben nach der Verschlüsselung	D	J	K	L	N	O	P	Q

Die in Rot geschriebenen Buchstaben gehören zum Schlüsselwort. Da doppelte Buchstaben weggelassen werden müssen, werden das E, das H und das I beim zweiten Auftreten übersprungen.

In grün findest du die restlichen Buchstaben, die nach den Regeln aufgefüllt werden.

Mit dieser Tabelle können die Geschwister nun ihre Nachrichten verschlüsseln. Amelie erstellt sich mit Hilfe des Schlüsselworts die gleiche Tabelle und kann so den Gemeintext entschlüsseln.

Übung: Erstelle eine Tabelle zum Schlüsselwort „Student“!

Verschlüsseln durch Änderung der Reihenfolge im Wort (Transposition)

Henrik hat eine neue Art der Verschlüsselung entdeckt, die Transposition. Dabei wird die Position eines Buchstabens in einem Wort oder einem Satz verändert.

Er erklärt es Lena am Wort „S c h i f f f a h r t“.

Bei der Transposition muss man folgendermaßen vorgehen:

1. Die Buchstaben des Worts werden auf zwei Zeilen aufgeteilt, wobei Buchstaben an ungeraden Stellen im Wort (erste, dritte, fünfte Stelle und wo weiter) in der oberen Zeile stehen, alle an gerader Stelle (zweite, vierte, sechste Stelle und so weiter) in der zweiten Zeile. Du schreibst den ersten Buchstaben also in die obere Zeile, den zweiten in die zweite Zeile, den dritten wieder in die erste Zeile und so weiter.

S h f f h t

c i f a r

2. Die Zeichenkette aus Zeile 2 wird an Zeile 1 angehängt.

Es entsteht als Geheimtext „Shffhtcifar“.

Wenn du damit ganze Sätze verschlüsseln willst, kannst du die Wörter des Satzes auch im Geheimtext mit Leerzeichen trennen.

Entschlüsseln eines solchen Geheimtext

1. Wir schauen uns an, wie lange das verschlüsselt Wort ist. Unser Geheimtext „Shffhtcifar“, hat 11 Zeichen. Da die Buchstaben beim Verschlüsseln immer abwechselnd in die erste und zweite Zeile geschrieben werden, muss die obere Zeile 6 Buchstaben, die untere Zeile 5 Buchstaben lang sein.

Es entsteht:

S h f f h t

c i f a r

2. Zum Entschlüsseln lese im Wechsel immer einen Buchstaben auf der oberen Zeile und einen aus der anderen Zeile, wie es die Pfeile zeigen.

Übung:

A) Verschlüssle das Wort „Garten“ mit Hilfe der Transposition!

B) Entschlüssle den Geheimtext „Shkldcooae im Böcerthn“ und finde heraus, was das Lieblingsessen von Lena ist.

Verschlüsselung von Zahlen

Lena und Henrik wollen Amelie ihre Telefonnummer geben, aber auch diese soll für andere geheim bleiben.

Frage: Welche Wege fallen dir ein, um die Telefonnummer zu verschlüsseln!

Idee 1: Wir nutzen eine einfache Rechenvorschrift zum Verschlüsseln

Die Geschwister ziehen von jeder Ziffer ihrer Telefonnummer eine Ziffer ab, nur die Null bleibt erhalten.

Telefonnummer: 012345 67890

Verschlüsselt: 001234 56780

Idee 2: Verschlüsseln mit einer Ziffernfolge:

Die Ziffern aus dem Code werden zu den Ziffern der Telefonnummer dazugezählt (addiert), so dass eine neue Zahl entsteht. Tipp: Leerzeichen helfen beim besseren lesen.

Telefonnummer: 0 1 2 3 4 5 6 7 8 9 0

Code: 5 2 3 4

Berechnung:

0 + 5 = 5

1 + 2 = 3

2 + 3 = 5

4 + 4 = 8

5 +5 = 10

6 +2 = 8 und so weiter

Verschlüsselte Telefonnummer: 5 3 5 8 10 8 10 12 14 2

Tipp: Du kannst zum Verschlüsseln, alle Rechenarten anwenden! Du kannst den Code addieren (+), subtrahieren (, abziehen, -), multiplizieren (mal) und dividieren (geteilt).

Übungen: Die Zahlenfolge 8 5 9 4 4 5 wurde nach dem Verfahren aus dem Beispiel mit dem Code 413 verschlüsselt. Wie lautet die ursprüngliche Zahl?

Die Geheimschrift

Lena und Henrik wollen ihr größtes Geheimnis sicher aufschreiben. Alle bisherigen Verschlüsselungen sind ihnen aber nicht sicher genug. Deshalb überlegen sie sich einige eigene Geheimschrift.

Dazu ordnen sie jedem Buchstaben ein Symbol zu.

A	B	C	D	E	F	G	H	I	J
☺	€	….	---				??		

Statt „dach“ können sie nun ---☺…?? schreiben

Aufgabe: Überlege dir selbst eine eigene Geheimschrift aus Symbolen! Schreibe damit eine Nachricht und lass sie jemand anderes entschlüsseln!

Wichtig, der Partner muss dazu deine Tabelle mit den Zeichen haben.

Symmetrische und asymmetrische Verschlüsselungen

Die Verschlüsselungen, die dir Henrik und Lena bisher vorgestellt haben, gehören zur Art der **symmetrischen Verschlüsselungen**. Von symmetrisch spricht man, wenn beide Seiten gleich sind. Das bedeutet Sender und Empfänger nutzten den gleichen Schlüssel, um die Nachricht zu verschlüsseln und wieder zu entschlüsseln.

Frage: Welches Problem besteht bei dieser Art der Verschlüsselung?

Lösung: Die Partner müssen die Schlüssel austauschen, dabei können sie andere in Erfahrung bringen. Wenn beispielsweise Henrik und Lena Amelie einen Zettel mit dem Schlüssel geben und jemand Amelie beim Lesen des Zettels unbemerkt über die Schulter, kennt dieser den Schlüssel und kann die Nachrichten entschlüsseln.

Hier helfen **asymmetrische Verschlüsselungen**. Dabei gibt es einen öffentlichen Schlüssel, den jeder kennt. Damit kann die Nachricht verschlüsselt aber nicht mehr entschlüsselt werden. Zum Entschlüsseln braucht der Empfänger seinen geheimen Schlüssel, den nur er kennt.

Zum Entschlüsseln wird dann der verschlüsselte Text durch Berechnungen entschlüsselt. Asymmetrische Verfahren sind viel sicherer, aber auch viel schwieriger zu berechnen. Das übernehmen heute Computer.

Wie sicher sind Verschlüsselungen?

Jede Verschlüsselung kann durch häufiges Ausprobieren möglicher Verschlüsselungsmethoden und Schlüssel geknackt werden!

Es ist aber eine Frage des Aufwands. Braucht der beste Computer, den es aktuell gibt, hunderte Jahre zum Entschlüsseln, gilt das Verfahre als sicher, denn so lange kann keiner warten.

Allgemein gilt: Je länger der Schlüssel, desto sicherer ist die Verschlüsselung.

Beim Entschlüsseln vor allem einfacher Verschlüsselungen helfen Häufigkeitstabellen:

In deutschen Wörtern kommen Buchstaben wie e und n sehr häufig vor. Tauchen im Geheimtext andere Buchstaben sehr häufig ein, ist es wahrscheinlich, dass diese für n oder e stehen.

Beispiel:

Wir verschlüsseln das Wort „Lernen“ mit der Caesar-Chiffre und der Verschiebung um 1.

Es entsteht: „Mfsofo“. Man sieht, die Buchstaben f und o kommen häufiger vor als die anderen Buchstaben.

Steganographie – Nachrichten werden versteckt

Bei der Steganographie bleiben die Nachrichten im Klartext. Sie werden jedoch versteckt. Beispielsweise wurde Seidenstoff beschriftet, in Wachskügelchen eingetaucht und geschluckt. Es wurden Schweineblasen beschrieben und in eine Flasche gesteckt, die danach mit Wein gefüllt wurde. auch unsichtbare Geheimtinten (siehe weiter hinten im Studienbrief) wurden verwendet. Während des Zweiten Weltkrieges nutzten Geheimagenten für ihre Nachrichten „Mikropunkte“. Die Texte wurden fotografiert und ihr Foto auf einen Millimeter verkleinert. Dieser Text in Form eines „Mikropunkts“ wurde auf einem unscheinbar wirkenden Dokument versteckt und viel so gar nicht auf. Auch wurden die Botschaften in anderen Texten versteckt. Das Problem war, wer Verfahren der Stenographie kannte, entdeckte die versteckten Texte ziemlich leicht. Deshalb entwickelten die Menschen schon sehr früh Verfahren zur Kryptografie.

Stenographie in einem Text

Frage: Kannst du die Geheime Nachricht in folgendem Text finden?

Tipp: Denke an die 3!

Folgender Text stammt aus dem Buch:

Franz Frühmann: Die dampfenden Hälse der Pferde im Turm von Babel (Hinstorff, 2005)

Liebste Eltern!

Macht euch keine Sorgen um uns, die währen wirklich unbegründet.
Es währe ganz falsch, wenn ihr denken würdet,
gute Eltern, Hänsel und Gretel sind in der Gewalt einer Hexe!
Wir leben hier bei einer sehr netten alten Dame, die uns jeden Wunsch von den Augen abliest! Zuerst dachte Gretel ja,
wir werden gefangen gehalten und sollten geschlachtet werden! Geht denn so was zu fassen! Wir haben uns dusselig gelacht! Es gibt hier viele Tiere, vor allem Vögel, die fliegen gewöhnlich
bis zur großen Eiche und dann in Richtung Norden, dort liegt nämlich ihr Futterplatz. Wir haben auch sehr schöne Puppen, mit denen wir spielen, und dazu viele Einrichtungen, so etwa auch
ein Kuchenhaus mit einem Dach aus Schokolade und Marzipan.
Einmal spielten wir Kasperletheater, da haben Löwen die Kaspers auf einen Baum gejagt und da schrien sie: He da ihr Förster!
Hier sind wir! Kommt rasch und rettet uns! Eure unglücklichen Dienstzeiten, ihr Waldwächter, sind unmöglich! Ihr müsstet mittags jagen, anstatt Amtspausen zu halten und zu pennen! Eure
Kinder Hänsel und Gretel bitten euch darum, nicht länger zu sorgen, teuerste Eltern! Uns geht`s vorzüglich. Gestern durfte Gretel ein Kleid der lieben alten Dame mit einem rosa Band umsäumen. Vielleicht, sie sprach schon davon, schlachtet morgen die liebe alte Dame ein Gänslein für uns oder sie spielt mit uns wieder Theater. Gestern schenkte sie gar von ihren Marionetten die
Hexe Hänsel. Es klingt unglaublich und ist doch die Wahrheit.
Dürfen wir dies denn auch annehmen? fragten wir, doch die Gute nickte. Nun will sie mit uns spazieren gehen und ruft uns zu:
Eilt! Eilt! Es ist höchste Zeit! Wo bleibt ihr nur! Helft
eurer alten Dame den Mantel anzuziehen! So wollen wir jetzt schließen und bitten sehr: Seit sorglos und freut euch mit
euren Kindern.
Hänsel und Gretel

Die Zahl Drei liefert euch die Lösung. Lest nach der Anrede „Liebe Eltern!“ nur jede dritte Zeile des Brieftexts!

Liebste Eltern!

Macht euch keine Sorgen um uns, die währen wirklich unbegründet.
Es währe ganz falsch, wenn ihr denken würdet,
gute Eltern, Hänsel und Gretel sind in der Gewalt einer Hexe!
Wir leben hier bei einer sehr netten alten Dame, die uns jeden Wunsch von den Augen abliest! Zuerst dachte Gretel ja,
wir werden gefangen gehalten und sollten geschlachtet werden! Geht denn so was zu fassen! Wir haben uns dusselig gelacht! Es gibt hier viele Tiere, vor allem Vögel, die fliegen gewöhnlich
bis zur großen Eiche und dann in Richtung Norden, dort liegt nämlich ihr Futterplatz. Wir haben auch sehr schöne Puppen, mit denen wir spielen, und dazu viele Einrichtungen, so etwa auch
ein Kuchenhaus mit einem Dach aus Schokolade und Marzipan.
Einmal spielten wir Kasperletheater, da haben Löwen die Kaspers auf einen Baum gejagt und da schrien sie: He da ihr Förster!
Hier sind wir! Kommt rasch und rettet uns! Eure unglücklichen Dienstzeiten, ihr Waldwächter, sind unmöglich! Ihr müsstet mittags jagen, anstatt Amtspausen zu halten und zu pennen! Eure
Kinder Hänsel und Gretel bitten euch darum, nicht länger zu sorgen, teuerste Eltern! Uns geht`s vorzüglich. Gestern durfte Gretel ein Kleid der lieben alten Dame mit einem rosa Band um-
säumen. Vielleicht, sie sprach schon davon, schlachtet morgen die liebe alte Dame ein Gänslein für uns oder sie spielt mit uns wieder Theater. Gestern schenkte sie gar von ihren Marionetten die
Hexe Hänsel. Es klingt unglaublich und ist doch die Wahrheit.
Dürfen wir dies denn auch annehmen? fragten wir, doch die Gute nickte. Nun will sie mit uns spazieren gehen und ruft uns zu:
Eilt! Eilt! Es ist höchste Zeit! Wo bleibt ihr nur! Helft eurer alten Dame den Mantel anzuziehen! So wollen wir jetzt schließen und bitten sehr: Seit sorglos und freut euch mit
euren Kindern.
Hänsel und Gretel

Aufgabe:

Versucht selbst eine Nachricht zu erstellen, in der eine Botschaft versteckt ist.

Denkt dabei daran, der ganze Text muss einen Sinn ergeben, wie im obigen Brief.

Geschichte der Verschlüsselung

Schon 3000 Jahre vor Christus Geburt, also vor mehr als 5000 Jahren, gab es in Ägypten erste Verschlüsselungsmethoden. Seither werden damit Nachrichten geschützt.

Die Enigma – eine der bekanntesten Verschlüsselungsmaschinen

Eine der berühmtesten Verschlüsselungsmaschinen des 20. Jahrhundert ist die Enigma. Durch ihre Hilfe konnten die Deutschen im zweiten Weltkrieg lange die Informationen für ihre Funksprüche verschlüsseln und sich so einen Vorteil gegenüber ihren Gegnern verschaffen.

Die Enigma und zwei Schlüsselwalzen (links). Quelle: Wikipedia.de / William Warby from London, England - Enigma, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=46848023

Der Name Enigma stammt vom altgriechischen Begriff für Rätsel („ainigma“) ab. Erfunden wurde sie vom Unternehmer und Ingenieurs Arthur Scherbius. Er lebte von 1878-1929. Die vielen Jahrtausende zuvor war das Ver- und Entschlüsseln von Nachrichten aufwendige Handarbeit. Im Ersten Weltkrieg hatte sich zudem gezeigt, dass eine Verschlüsselung bei der einfach ein Buchstabe gegen einen anderen ausgetauscht wird Schwächen hat. Scherbius und andere Wissenschaftler lösten dieses Problem, indem sie eine „polyalphabetischen Verschlüsselung“ einsetzten. Der Wortteil „poly“ steht für „viel.“ So wird ein Buchstabe nicht jedes Mal auf den gleichen Buchstaben geändert, sondern immer auf einem anderen Buchstaben. Die Enigma nutzte dazu auf einfachen Stromkreisen. Diese verbanden die Taste mit dem Buchstaben des Tastenfelds mit einem Lämpchen, das auf dem Anzeigenfeld den Buchstaben des Geheimtexts aufleuchten ließ. Der Stromkreis führt durch verschieden Walzen, die durch ihre Stellung bestimmen, welcher Buchstabe für eine Taste aufleuchtet.

Zum Entschlüsseln brauchte der Empfänger ebenso eine Enigma und Informationen darüber, wie die Walzen eingestellt waren. Diese wurden auf verschiedenen Wegen mitgeteilt. Im Jahr 1940 gelang es den Engländern jedoch den Code zu knacken, damit war die Erfolgsgeschichte der Enigma zu Ende.[1]

Hashwertverfahren – Wo her weiß ich, dass mein Dokument auf dem Weg nicht verändert wurde?

Nicht immer müssen Henrik und Lena ihre Nachrichten verschlüsseln. So senden sie eine unverschlüsselte E-Mail an Amelie mit einer Einladung zum Geburtstag. Sie wollen aber sicher gehen, dass niemand beim Transport der E-Mail über das Internet den Text verändert, ohne dass es Amelie merkt. Deshalb teilen Sie Amelie einen „Hashwert“ mit, mit dem sie die Nachricht prüfen kann.

Ein Hashwert ist eine Zahl mit fester Länge, die aus dem Text heraus berechnet wird und sicherstellt, dass der Text auch genauso ankommt, wie er beim Berechnen des Hash aussah. Jeder Text hat einen eindeutigen Hashwert, den kein anderer Text auf der Welt hat.

Normalerweise wird der Hashwert nicht aus den Buchstaben selbst berechnet, sondern aus ihren digitalen Daten, denn jeder Computer wandelt Buchstaben zum Verarbeiten in einer Folge von 0 und 1 um.

Da Lena und Henrik aber den Wert von Hand berechnen wollen, überlegen sie sich ein eigenes einfaches Verfahren.

[1] Die ausführliche Erklärung der Funktionsweise der Enigma und der Weg wie ihre Verschlüsselung geknackt wurde findest du unter:
https://www.wissen.de/wie-der-code-der-legendaeren-enigma-maschine-geknackt-wurde

Der Algorithmus dazu geht so:

1. Zähle die Buchstaben, die in jedem Wort vorkommen!

2. Schreibe die Anzahl der Buchstaben je Wort hintereinander!

3. Addiere alle Wortlängen zu einer Prüfzahl und schreibe sie ans Ende.

Der Einladungstext der Geschwister lautet:

„Wir feiern am Montag um vierzehn Uhr bei uns!“

Schritt 1 und 2 (Wortlängen): 3 6 2 6 2 8 3 3 3

Schritt 3: Prüfzahl: 3+6+2+6+2+8+3+3+3 = 36

Hash: 36362628333

Würde jetzt jemand den Montag gegen Dienstag austauschen, ändert sich der Hash zu: 38362828333, da Dienstag 8 Zeichen hat, Montag nur 6.

Wichtig: Der Hash aus dem Beispiel funktioniert bei diesem speziellen Text. Er sichert nicht bei allen Texten, dass diese nicht verändert wurden.

Wo kommt Verschlüsselung zum Einsatz?

Henrik und Lena verschlüsseln Botschaften untereinander und an ihre Freunde. Verschlüsselungen kamen in vielen Kriegen zum Einsatz. Sie finden aber auch im Alltag Anwendung.

In folgenden Bereichen findest du beispielsweise Verschlüsselungen:

- Verschlüsselte Datenübertragung im Internet
- Verschlüsselte Dateien auf dem eigenen Computer
- bei Banken

Mehr dazu erfährst du im Lernvideo.

Geheimtinte für geheime Botschaften

Henrik und Lena haben bisher nur ihre Nachrichten verschlüsselt. Sie wollen aber noch einen Schritt weitergehen und nun auch die Nachrichten unsichtbar machen.

Dazu nutzen sie verschiedene Geheimtinten, die hier nun kennenlernt.

1. Geheimtinte die man mit Wärme sichtbar machen kann:

- Zitronensaft
- Orangensaft
- Apfelsaft
- Zwiebelsaft
- Essig
- Milch
- Zuckerwasser

Die Nachricht wird mit einem Pinsel oder Wattestäbchen mit der Geheimtinte auf ein weißes Papier geschrieben. Ist sie getrocknet ist sie unsichtbar.

Um sie sichtbar zu machen, erwärmt man das Blatt ganz vorsichtig, zum Beispiel mit einem Bügeleisen (lass dir dabei eventuell von einem Erwachsenen helfen).

Der Kohlenstoff, der in der Geheimtinte vorhanden ist, verkohlt, der Text wird sichtbar.

2. Geheimtinte, die man chemisch sichtbar machen kann

- Zitronensaft
- Natron in Wasser aufgelöst
- Essig

Die Nachricht wird mit einem Pinsel oder Wattestäbchen mit der Geheimtinte auf ein weißes Papier geschrieben. Ist sie getrocknet ist sie unsichtbar.

Zum Sichtbarmachen von Zitronensaft und Essig brauchst du Rotkohllösung

Zur Herstellung der Rotkohllösung kochst du einfach frischen Rotkohl in Wasser, bis sich dieses kräftig färbt. Pinsle damit das Blatt ein.

Natronlösung kannst du mit Traubensaft sichtbar machen.

Wie funktioniert das?

Rotkohl und Traubensaft enthalten Farbstoffe die als Indikatoren wirken. Indikatoren sind Substanzen, die ihre Farbe verändern, wenn sie mit Säure (zum Beispiel Essig oder Zitronensaft) oder einer Lauge (zum Beispiel Natronlösung) in Kontakt kommen.

Zum Weiterlesen und weiter Forschen

Internetseiten

Zur Geschichte der Kryptographie:

https://www.welt.de/print/wams/wissen/article106298767/Geschichte-der-Kryptografie.html

https://www.bpb.de/apuz/259145/eine-kurze-geschichte-der-kryptografie

Die Funktionsweise der Enigma:

https://www.wissen.de/wie-der-code-der-legendaeren-enigma-maschine-geknackt-wurde

Krypto im Advent – jeden Tag im Advent interessante Rätsel rund um die Verschlüsselung:

https://www.krypto-im-advent.de

Liste von Programmen und Möglichkeiten eure Daten auf PC und Smartphone und eure Nachrichten zu verschlüsseln:

https://www.studioimnetz.de/projekte/watchingyou/verschluesselung/

Informationen zu Julius Caesar:

https://www.geo.de/geolino/mensch/8983-rtkl-rom-er-kam-sah-und-siegte-julius-caesar

https://www.kinderzeitmaschine.de/antike/rom/lucys-wissensbox/alltag/drei-namen-fuer-einen-roemer/

Bastelanleitungen und Vorlage zum Ver- und Entschlüsseln der Caesar-Chiffre:

https://www.kindernetz.de/infonetz/laenderundkulturen/geheimschriften/-/id=25340/property=download/nid=22494/1vpb4gn/index.pdf

Ausflugziele

Deutschen Spionagemuseum Berlin

https://www.deutsches-spionagemuseum.de

Mathematikum Gießen mit Sonderaustellung zur Kryptografie:

https://www.mathematikum.de

Lösungen zu den Übungen

Caesar-Chiffre:

A:

garten

geheimnis

schokoladeneis

B:

kdoor phlq qdph lvw dpholh.

Verschlüsslung mit einem Zahlencode

A: dmdw

B: mond

C: 317

Verschlüsseln mit einem Codewort oder Schlüsselsatz durch Verschieben

Der Geheimtext lautet Lbg Znadvxws jgc ru Tqaaioy

Alphabetische Verschlüsselung

A: tpbs

b: auto

Austauschen von Buchstaben auf Basis eines Schlüsselworts

Schlüsselwort. Student

Buchstaben im Klartext	A	B	C	D	E	F	G	H	I
Buchstaben nach der Verschlüsselung	S	T	U	D	E	N	V	W	X

Buchstaben im Klartext	J	K	L	M	N	O	P	Q	R
Buchstaben nach der Verschlüsselung	Y	Z	A	B	C	F	G	H	I

Buchstaben im Klartext	S	T	U	V	W	X	Y	Z
Buchstaben nach der Verschlüsselung	J	K	L	M	O	P	Q	R

Verschlüsselung von Zahlen

Klartext: 4 4 6 0 3 2

Du musst die Ziffern des Code von den Ziffern der verschlüsselten Zahl abziehen.

Transposition

A: Greatn

B: Schokolade im Brötchen