Was ist Kryptografie und warum ist sie so wichtig?

Unterrichtseinheiten zum Thema Daten verschlüsseln und entschlüsseln

4 – 6 Lektionen

Beschreibung der schulischen Situation

Die Unterrichtseinheit habe ich für Klassen der ersten Oberstufe im Fach Medien und Informatik geplant. Sie kann auf Sek- und Realschulniveau durchgeführt werden. In vorangehenden Lektionen wurde die Kommunikation anhand des Buches Connected 2 behandelt. Auf der Realschulstufe hat es 15 Schülerinnen und Schüler pro Klasse, auf der Sekundarstufe sind es 23 Schülerinnen und Schüler. Die Jugendlichen besuchen eine Lektion pro Woche den Medien- und Informatikunterricht.

Geschichte und Grundbegriffe

Mit der Entwicklung der Schriften wurden erstmals schriftliche Mitteilungen zu Elementen einer Art Geheimsprache. Lesen und Schreiben unterrichteten meistens Priester unterschiedlicher Religionen. Jegliche Schrift basiert auf einer endlichen, nichtleeren Menge von ausgewählten Zeichen, die Alphabet genannt wird. Die Zeichen des Alphabets nennen wir auch Symbole oder Buchstaben. Ursprünglich stellten viele Zeichen Gegenstände und Tiere dar, mit der Zeit wurden diese immer stärker vereinfacht, bis sie schliesslich symbolischen Charakter annahmen. Die schriftlichen Mitteilungen erhält man, wenn man die Symbole in einer Folge anordnet. Diese Symbolfolgen nennen wir Texte.

Mit der sozialen Entwicklung der Gesellschaften war der Fortschritt in Bezug auf Lese- und Schreibkenntnisse dann aber nicht mehr zu bremsen, und der Anteil der Bevölkerung mit Schreibfähigkeit stieg stark an. In dieser Zeit entstand auch der Bedarf an der Entwicklung der Geheimschriften.

Dieses Schema zeigt den Kommunikationsschritt, bei dem der Sender dem Empfänger einen Geheimtext schickt. Die Übertragung des Geheimtextes wird durch ein Übertragungsmedium (zum Beispiel einen Boten oder das Internet erfolgen.

Das oben abgebildete Schema nennen wir Kommunikationsschema. Hier wollen zwei Leute schriftlich eine geheime Nachricht austauschen, wobei die Nachricht ein Text in einer natürlichen Sprache ist. Es kann in folgende Kommunikationsschritte zerlegt werden:

In einem Kommunikationsschritt schickt der Sender die Nachricht an den Empfänger. Diese Nachricht ist in einer Sprache verfasst, die beide verstehen, und sie wird im Folgenden mit Klartext bezeichnet.

Die Rollen des Senders und Empfängers sind für einen Kommunikationsschritt fest zugeteilt und können erst in einem weiteren Kommunikationsschritt neu verteilt werden. Beim Übertragen der Nachricht müssen Sender und Empfänger immer damit rechnen, dass etwas schiefgeht. Beispielsweise könnten sie es mit einem unzuverlässigen Boten zu tun haben oder sogar mit einem Gegner, der ihnen schaden will. Sender und Empfänger wollen aber auf jeden Fall verhindern, dass jemand, der die geheime Nachricht in die Hände bekommt, diese lesen kann. Sie müssen sie also etwas einfallen lassen. Deshalb erstellen die beiden eine Geheimschrift, die nur sie beide kennen und die somit ihr gemeinsames Geheimnis ist. Eine solche Geheimschrift kann man als ein Paar von Algorithmen ansehen, die wir Chiffrierung und Dechiffrierung nennen.

Die Chiffrierung ist ein Verfahren, das einen Klartext in einen Geheimtext umwandelt. Die Dechiffrierung ist ein Verfahren, welches das Ganze wieder rückgängig macht, nämlich einen Geheimtext in den Klartext zurückverwandelt. Der Geheimtext wird vom Sender mit Hilfe eines Übertragungsmediums zum Empfänger geschickt. Das Internet ist ein aktuelles Beispiel für ein solches Übertragungsmedium. Es stellt eine sehr zuverlässige Nachrichtenübertragung dar, denn jede E-Mail, die unverschlüsselt übers Internet gesendet wird, kann ohne weiteres abgefangen und gelesen werden. Mails können mit Postkarten verglichen werden. Weil sie in keinem Briefumschlag sind, könnte jede Person, welche die Postkarte in die Hände bekommt, die Nachricht auch gleich lesen.

Die Klartexte sind Folgen von Buchstaben eines Alphabets derjenigen Sprache, die für die Kommunikation verwendet wird. Im Medien- und Informatikunterricht wird die deutsche Sprache verwendet und dazu gehört das lateinische Alphabet.

Lat = { 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 }.

Es wird in den meisten europäischen Sprachen benutzt. Leerzeichen, Punkte, Kommas und alle anderen Interpunktionszeichen werden im Klartext nicht verwendet. Sie werden deshalb weggelassen. Oft wird auch nicht zwischen Gross- und Kleinbuchstaben unterschieden, es werden nur Texte verwendet, die aus Grossbuchstaben bestehen. Für das Alphabet des Geheimtextes können beliebige Buchstaben, Zahlen oder andere bereits bestehende, aber auch selbst erfundene Symbole verwendet werden. Die Länge eines Textes ist die Anzahl der Zeichen der Buchstabenabfolge. Somit ist die Länge des Textes *ANNA* genau vier.

Kryptosysteme

Dieses Kommunikationsschema zeigt den Kommunikationsschritt, bei dem die Übertragung einer verschlüsselten Nachricht gezeigt wird. Um den Klartext zu verschlüsseln oder den Kryptotext zu entschlüsseln, brauchen beide Kommunikationspartner einen gemeinsamen geheimen Schlüssel.

Die Geheimschriften basieren auf einem gemeinsamen Geheimnis der kommunizierenden Personen. Dieses Geheimnis ist die «Art und Weise» der Chiffrierung, die üblicherweise auch die «Art und Weise» der Dechiffrierung bestimmt. Keine dieser Geheimschriften kann jedoch lange verwendet werden, ohne dass man dabei ein Risiko eingeht, das Geheimnis zu lüften und damit den Geheimtext für einen Gegner lesbar zu machen. Deshalb wird eine grössere Vielfalt von Chiffrierungen innerhalb eines Chiffrierungssystems bevorzugt.

Anwendung der Kryptografie

Die folgende Liste nennt einige Möglichkeiten, erhebt jedoch keinen Anspruch auf Vollständigkeit:

- E-Mail: Verschlüsselte E-Mails sind ein klassischer Anwendungsbereich der Kryptografie.
- World Wide Web: Da das WWW für kommerzielle Portale und für Geschäftsprozesse genutzt wird, ist ein Kryptografie-Einsatz oft dringend geboten.
- Virtuelle Private Netze: Unternehmen mit mehreren Niederlassungen koppeln ihre lokalen Netze oft über das Internet. Es lohnt sich, alle Daten beim Verlassen eines Firmennetzes zu verschlüsseln, um sie bei Wiedereintritt in das Firmenterrain zu entschlüsseln. Diese Technik wird als VPN (Virtuelles Privates Netz) bezeichnet.
- Online-Bezahlsysteme: Das Online-Bezahlen ist ohne Zweifel eine Sache, die kryptografisch abgesichert werden sollte.
- Internet-Banking: Wozu zur Bank gehen, wenn man einen Internetanschluss hat? Aber bitte nur mit Kryptografie!

- Dateien: Nicht nur übertragene Informationen, sondern auch Daten, die auf einer Festplatte oder einem Dateiserver liegen, müssen geschützt werden.

Nach diesen einführenden Erklärungen folgen nun verschiedene Verschlüsselungsmethoden und die dazugehörenden Aufgaben für die Schülerinnen und Schüler. Dabei stehen die unten angeführten Lernziele im Vordergrund:

Die Schülerinnen und Schüler

- Können den Bedarf, Daten zu chiffrieren und zu dechiffrieren, nachvollziehen.
- kennen verschiedene Arten von Chiffrierungs- und Dechiffrierungsmechanismen und können diese anwenden: Kodierung von Buchstaben durch andere Buchstaben oder Wörter, durch Zeichen oder Symbole, Änderung der Positionen von Buchstaben im Text.
- erlernte Chiffrierungsmethoden modifizieren und kombinieren und somit eigene Geheimschriften und Kryptosysteme entwerfen und anwenden.
- mittels statistischer Häufigkeitsanalyse monoalphabetische Kryptosysteme knacken und Geheimtexte ohne Kenntnis des Schlüssels dechiffrieren.

Kompetenzen des Lehrplans 21

- MI 2.1c > Daten mittels selbst entwickelter Geheimschriften verschlüsseln
- MI 2.1d > analoge und digitale Darstellungen von Daten kennen und die entsprechenden Dateitypen zuordnen
- MI 2.2b > durch Probieren Lösungswege für einfache Problemstellungen suchen und auf Korrektheit prüfen
- MI 2.3n > Risiken unverschlüsselter Datenübermittlung und -speicherung abschätzen

Aufgabe 1

Geheimschrift mit Symbolen

Eine weit verbreitete Methode der Chiffrierung basiert auf der Kodierung der Buchstaben des Klartextes durch andere Symbole. Mit dieser Methode schaffst du es, eigene Geheimschriften zu entwickeln und anzuwenden.

Hier ein Beispiel einer Geheimschrift mit Symbolen, die ich den Buchstaben des lateinischen Alphabets zugeordnet habe.

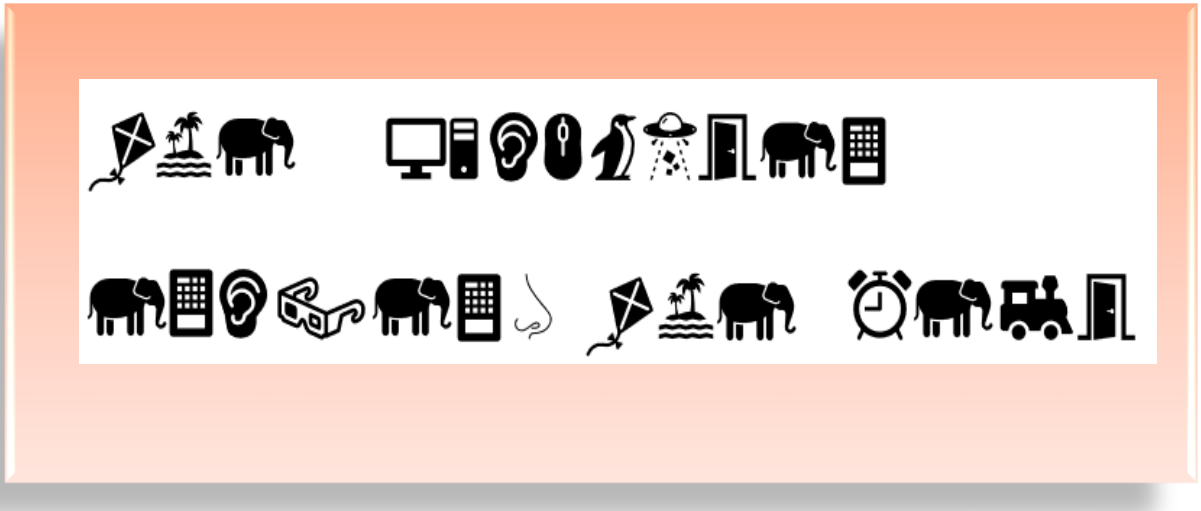
A 	H 	O 	V 
B 	I 	P 	W 
C 	J 	Q 	X 
D 	K 	R 	Y 
E 	L 	S 	Z 
F 	M 	T 	
G 	N 	U 	

Dabei habe ich darauf geachtet, dass das Symbol einen Wiedererkennungswert mit dem Buchstaben hat, zum Beispiel das  Symbol Apfel für den Buchstaben A.

Aufgabe 1
Geheimbotschaft dekodieren

5

Probiere die geheime Botschaft unten im Kasten zu entschlüsseln. Diese Übersetzung hilft dir dabei. Schreibe den Satz unten auf die Linie.



_____

Aufgabe 2
Geheimschrift erfinden

Denke dir eine eigene Geheimschrift aus. Zeichne rechts von den Buchstaben jeweils dein Geheimzeichen ins Kästchen.

Tipp: Je einfacher, desto besser. Du sollst nicht stundenlang für eine kurze Mitteilung brauchen, andererseits soll der Empfänger nicht genauso lange an der Entschlüsselung haben.

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

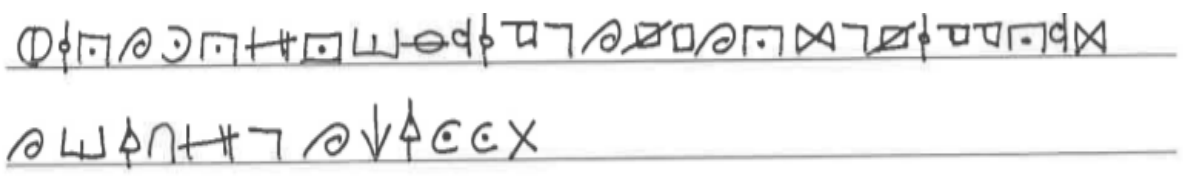
Aufgabe 3
Geheimbotschaft schreiben

Schreibe eine verschlüsselte Botschaft mit deiner Geheimschrift.

Jetzt folgt ein weiteres Beispiel für eine Geheimschrift mit Symbolen. Hier habe ich für jeden Buchstaben ein Symbol gezeichnet.

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		SCH		SP		ST		CK	
EI		AU		leer		?		.	

Aufgabe 4
Versuche diesen Text zu entschlüsseln.
Schreibe die Lösung auf die Linien.



Aufgaben Verschlüsseln mit Cäsar

Das einfachste, das in der Antike vom römischen Feldherrn Gaius Julius Caesar verwendet wurde, ist CAESAR. Dieses System nutzt die Möglichkeit, die Symbole des lateinischen Alphabets in einer festen Ordnung aufzulisten. Jeder Buchstabe des Klartextes wird durch einen anderen Buchstaben im Geheimtext codiert. Vor der Ausführung der eigentlichen Kommunikation einigen sich der Sender und der Empfänger auf einen geheimen Schlüssel. Der Schlüssel ist eine Zahl $i \in \{0.1, \ldots.25\}$ und wird als Abstand (in der Auflistung der Symbole des Alphabets) zwischen den Buchstaben des Klartextes und den entsprechenden Buchstaben im Geheimtext betrachtet.

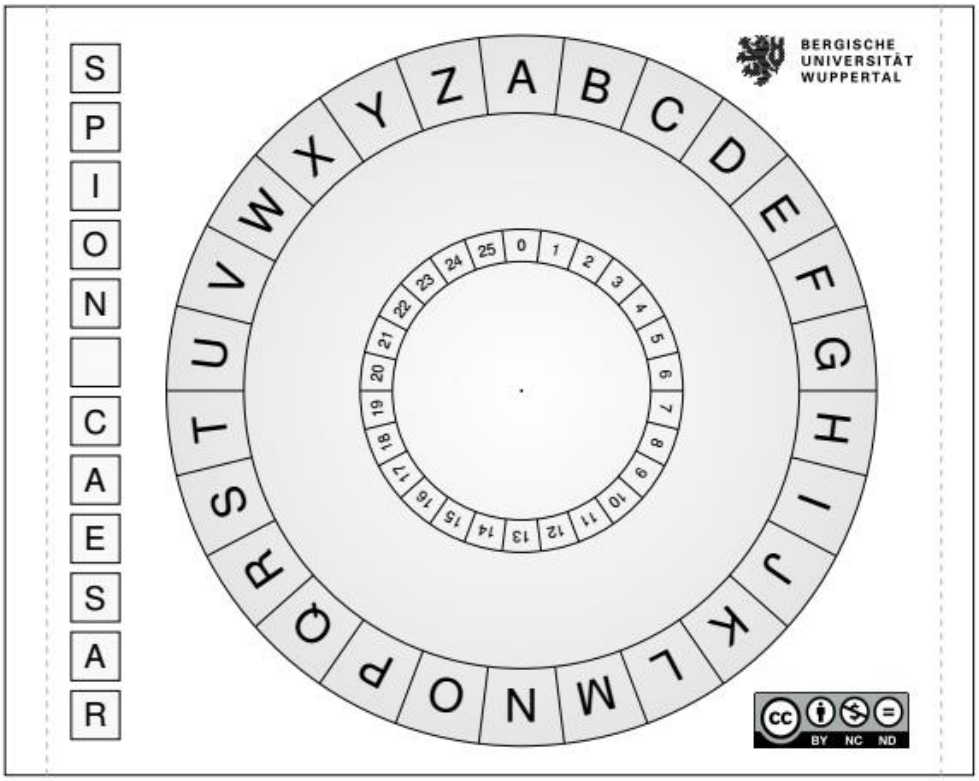
Wenn der Schlüssel zum Beispiel i = 3 ist, dann wird A mit Ord(A) = 0 unabhängig von seiner Position im Klartext durch den Buchstaben D mit Ord(D) = 3 codiert, eil Ord(D) – Ord(A) = 3. Weiter wird B durch E, Cdurch F usw. codiert. Für die letzten drei Buchstaben X, Y und Z mit Ord(X) = 23, Ord(Y) = 24 und Ord(Z) = 25 werden

zur Codierung die noch freien Symbole A, B und C verwendet. Man geht für die Codierung also wieder an den Anfang des Alphabets zurück.

Verschlüsselung mit Schlüssel 9

Das Kryptosystem CAESAR hat 26 Schlüssel und enthält damit 26 Geheimschriften, jeweils eine pro Schlüssel. Natürlich lohnt es sich nicht den Schlüssel mit dem Wert 0 zu verwenden, weil dann der Geheimtext identisch mit dem Klartext ist.

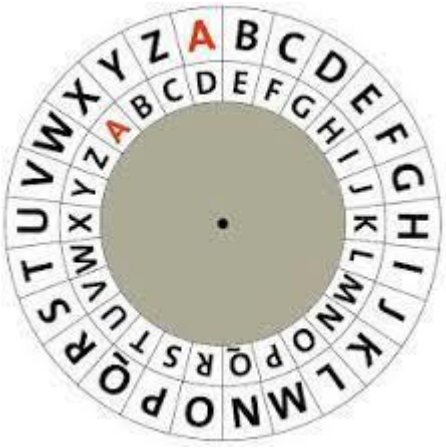
Auf der folgenden Seite findet man eine Chiffrierscheibe. Mit diesen beiden Scheiben kann die Ver- und Entschlüsselung mit CAESAR einfach ausgeführt werden. Der Schlüssel bestimmt die Anzahl der Buchstaben, um die die innere Scheibe im Gegenuhrzeigersinn gedreht wird. Danach werden die Klartextbuchstaben auf der äusseren Scheibe durch die Geheimtextbuchstaben der inneren Scheibe codiert.



Die Caesar-Verschlüsselung kann leicht geknackt werden. Man muss maximal 25 Schlüssel durchprobieren, um den Klartext zu erhalten. Schwieriger wird es, wenn das Verfahren mit einem Schlüsselwort kombiniert wird. Das funktioniert wie folgt:

Sender und Empfänger einigen sich auf ein Schlüsselwort.

Anschliessend wird das Alphabet mit den noch nicht benutzten Buchstaben, in alphabetischer Reihenfolge beim letzten Buchstaben des Schlüsselworts beginnend, aufgefüllt.



Im äusseren Ring der Scheibe steht
der **KLARTEXT**, im inneren Ring der **Geheimtext**.

Der **Schlüssel** gibt an, um wie viele Buchstaben der **Geheimtext** (innerer Ring) *gegen den Uhrzeigersinn* verschoben wurde.

Aufgabe 5

Verschlüssle das Wort **CAESAR** mit Schlüssel 5. Schreibe das Lösungswort auf die Linie.

_____

Differenzierung

10

Für schwächere Schülerinnen und Schüler gebe ich diese Hilfestellungen.

- Stelle die Buchstaben **A** und **a** aufeinander
- Wende Schlüssel 5 an: D.h. drehe die innere Scheibe um 5 Stellen *gegen den Uhrzeigersinn* (A und f liegen aufeinander)
- Gehe nun von *außen nach innen*: C --> h, A --> f, ...

  H F __ __ F __

Aufgabe 6

Verschlüssle den Text **VERSCHOBENEBUCHSTABEN** mit Schlüssel 9. Schreibe deine Verschlüsselung auf die Linie.

_____

Differenzierung für schwächere Schülerinnen und Schüler
Die ersten drei verschlüsselten Buchstaben sind gegeben.

E N A _____

Aufgabe 7

Entschlüssle diesen Text. Ü = UE
Der Schlüssel ist 5. Schreibe den entschlüsselten Text auf die Linie.

IFXNXYJNSJAJWXHMQZJXXJQYJSFHMWNHMY

_____

Differenzierung für stärkere Schülerinnen und Schüler

Der Schlüssel ist 14. Schreibe den entschlüsselten Text auf die Linie.

ROGWGHSWBSJSFGQVZISGGSZHSBOQVFWQVHRWSRISBHGQVZISGGSZHVOGH

_____

Aufgabe 8

Entschlüssle die folgenden Nachrichten. Mögliche Schlüssel sind: 7 oder 13.

YVRORE PNRFNE, VPU JREQR QN FRVA.

Differenzierung für stärkere Schülerinnen und Schüler

Entschlüssle die folgenden Nachrichten. Mögliche Schlüssel sind: 2, 7, 10 oder 13.

SPLIL RSLVWHAYH, AYLMMLU DPY BUZ ILP KLU WFYHTPKLU

Aufgaben Verschlüsseln mit Vigènere

Die Vigènere Verschlüsselung**,** ist ein polyalphabetisches Verschlüsselungsverfahren**,** das schon im 16. Jahrhundert verwendet wurde, um geheime Textnachrichten zu übermitteln.

Im Gegensatz zur Caesar Verschlüsselung wird bei dem Vigènere Verfahren nicht jeder Klartextbuchstabe um die gleiche Anzahl an Buchstaben verschoben. Stattdessen gibt es ein sogenanntes Schlüsselwort beziehungsweise Codewort. Den ersten Klartextbuchstaben verschlüsselt man dann mit dem ersten Buchstaben des Schlüsselwortes, den zweiten Buchstaben mit dem zweiten Buchstaben des Schlüsselwortes und so weiter. Ist das Schlüsselwort zu Ende, beginnt man wieder mit dem ersten Buchstaben.

Die Vigenère Verschlüsselung funktioniert wie folgt:

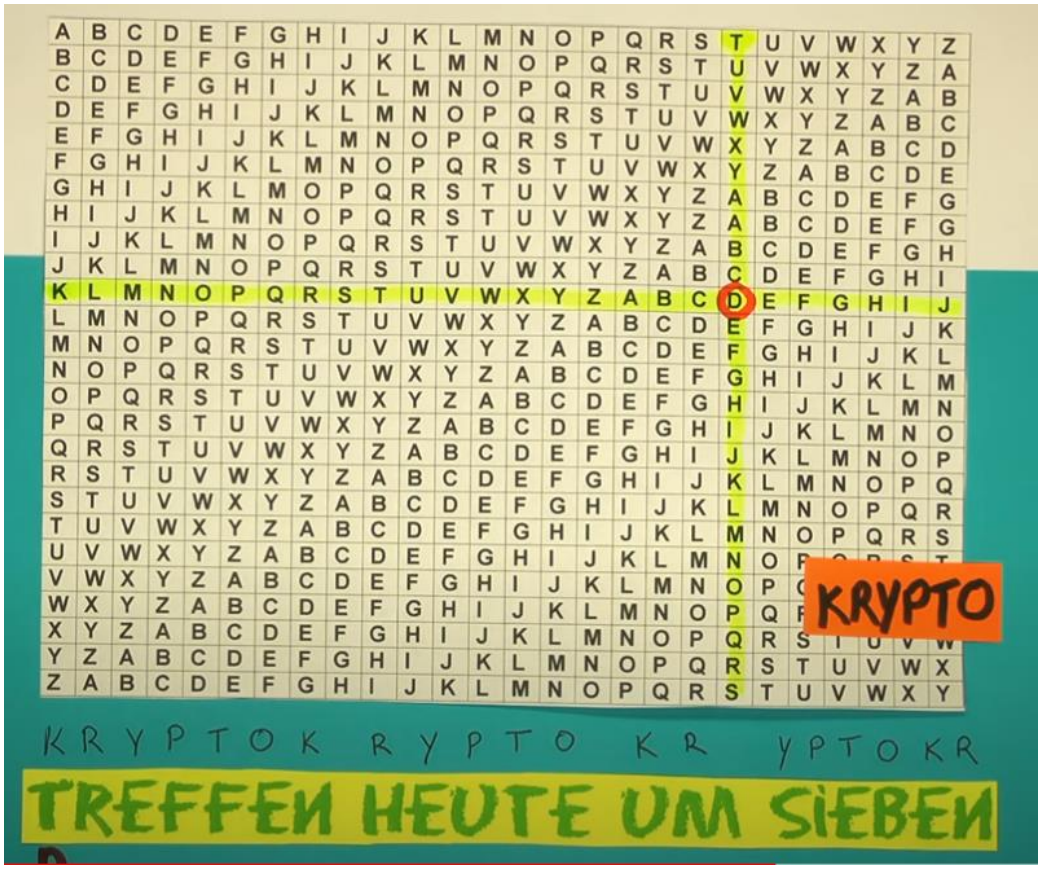
Sender und Empfänger einigen sich auf ein Schlüsselwort. Dieses wird unter die Nachricht geschrieben. Unter jeden Buchstaben der Nachricht wird ein Buchstabe des Schlüsselwortes geschrieben. Das Schlüsselwort wird dabei ständig wiederholt.

Klartext (KT): Ich bin ein sicherer Satz
Schlüsselwort (S): sicher

KT	I	C	H	B	I	N	E	I	N	S	I	C	H	E	R	E	R	S	A	T	Z
S	S	I	C	H	E	R	S	I	C	H	E	R	S	I	C	H	E	R	S	I	C

Beispiel einer Vigènere Verschlüsselung

Man nimmt sich jeweils einen Buchstaben der Nachricht und sucht ihn in der ersten Zeile des Vigenère-Quadrates (Klartextbuchstaben). Von da aus geht man nach unten bis zu der Zeile, in der sich ganz links der dazugehörende Buchstabe des Schlüsselwortes befindet. Beim Kreuzungspunkt der senkrechten und waagrechten Reihen befindet sich der verschlüsselte Buchstabe. In diesem Beispiel ist es D. Den Film habe ich als Einstieg in das Thema Verschlüsseln mit Vigènere gezeigt.



https://www.youtube.com/watch?v=4y4nCG8631g

KT	T	R	E	F	F	E	N	H	E	U	T	E	U	M	S	I	E	B	E	N
S	K	R	Y	P	T	O	K	R	Y	P	T	O	K	R	Y	P	T	O	K	R
VS	D	I	C	U	Y	S	X	Y	C	J	M	S	E	D	Q	X	X	P	O	E

Aufgabe 9

Erkläre mit dem untenstehenden Vigènere Quadrat wie das folgende Beispiel zustande kommt.

Klartext	G	E	H	E	I	M	N	I	S
Schlüsselwort	K	A	T	Z	E	K	A	T	Z
Geheimtext	Q	E	A	D	M	W	N	B	R

Schlüsselbuchstabe

Klartextbuchstabe

	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

Aufgabe 10

Verschlüssele den Klartext 'HALLOWIEGEHTS' mit dem Schlüssel 'ESEL'.
Schreibe die Lösung auf die Linie.

_____

Differenzierungsaufgabe für stärkere Schülerinnen und Schüler

Schreibe die Lösung auf die Linie.
Entschlüssele den Geheimtext 'LMSXEGXTXUS'. Der Schlüssel lautet 'ZEBRA'.

_____

Aufgabe 11

Wähle selbst einen Schlüssel. Verschlüssele einen Text mit dem Schlüssel. Gib den Geheimtext und den Schlüssel an deine Nachbarin / deinen Nachbarn zum Entschlüsseln weiter.

Zusammenfassung

Du hast gelernt, dass man einen lesbaren Text in einer natürlichen Sprache Klartext nennt. Wenn man den Text für andere unlesbar machen will, wandelt man ihn in eine Geheimsprache um. Das Resultat dieser Umwandlung wird Geheimtext genannt, die Umwandlung selbst nennt man Chiffrierung. Die Rekonstruktion des Klartextes aus dem Geheimtext nennt man Dechiffrierung.

Basis und Weiterführung zum Thema Geheimschriften

Die Schülerinnen und Schüler haben mit den erhaltenen Informationen und den dazu gestellten Aufgaben einen Einblick und kleinen Überblick des Themas der Chiffrierung und Dechiffrierung erhalten. Mit dem Erfinden einer eigenen Geheimschrift und deren Anwendung mit einer oder mehreren Aufgaben vertiefen sich die Schülerinnen und Schüler ein erstes Mal in diesem Themenbereich. In der zweiten Oberstufe wird das Thema der Codierung erneut aufgegriffen und behandelt.

Eine Codierung kann nicht nur bei textbasierten Inhalten angewendet werden. Zahlen und Zahlenkombinationen dienen ebenfalls der Verschlüsselung. Ich zeige diesen Inhalt anhand eines Smartphone-Codes auf.

Code eines Smartphones

Die sichere Speicherung und Übermittlung von Daten nimmt in der heutigen Gesellschaft einen immer grösseren Stellenwert ein. Grundkenntnisse der

Datensicherheit gehören heute zur digitalen Sozialisation und sind für das künftige Zusammenleben in der Gesellschaft von hoher Relevanz. Doch was bedeutet Sicherheit genau? Wählt man z.B. ein zufälliges 8- stelliges Passwort aus Gross- und Kleinbuchstaben sowie Ziffern (aber ohne Sonderzeichen), so ist dieses rund 4mal sicherer als ein zufälliges 8-stelliges Passwort nur aus Gross- und Kleinbuchstaben. Nimmt man aber eine Stelle mehr dazu und generiert ein 9-stelliges zufälliges Passwort, wird dieses rund 60mal sicherer. Deshalb trägt die Passwortlänge wesentlich zur Sicherheit eines Logins bei. Diese Inhalte und Aufgabenstellungen sollen Schülerinnen und Schüler anregen, sich mit der Datensicherheit auseinanderzusetzen.

Lernziele

Die Schülerinnen und Schülerinnen und Schüler können

- die Sicherheit eines Codes ihres Smartphones einschätzen.
- die Baumstruktur als systematische Darstellung von Möglichkeiten eines Codes (kartesisches Produkt; Kombinatorik) einsetzen.

Aufgabe 12

Du hast beobachtet, wie jemand seinen vierstelligen PIN-Code zum Entsperren des Smartphones eingegeben hat. Der Zahlencode beginnt mit einer 6, so viel konntest du gerade noch erkennen. Danach ging es zu schnell. Betrachte das Bild unten genau (siehst du die Fingerabdrücke?). Wie viele Möglichkeiten gibt es für den vierstelligen Zahlencode noch, wenn du die erste Ziffer kennst?

Antwort _____

Schreibe alle Lösungen auf, die es gibt:

Kleinste Zahl: 6 __ __ __

Zweitkleinste Zahl: 6 __ __ __

Drittkleinste Zahl: 6 __ __ __

Viertkleinste Zahl: 6 __ __ __

Fünftkleinste Zahl: 6 __ __ __

Grösste Zahl: 6 __ __ __

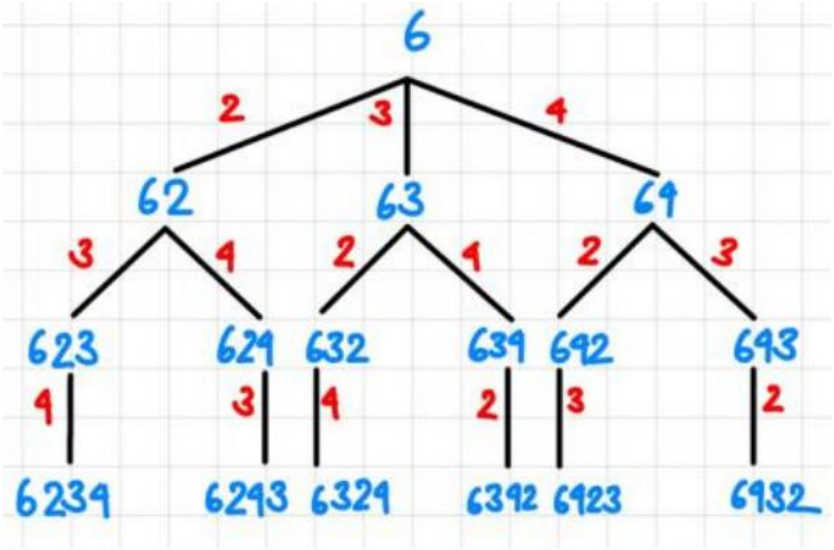
Aufgabe 13

Was denkst du, welches ist der richtige Code? Schaffst du es mit einem Versuch? Schreibe einen möglichen Code auf einen Zettel und zeige den Code deiner Lehrperson. Sie überprüft ihn und gibt dir weitere Anweisungen.

Der richtige Code lautet: 6 __ __ __

Anzahl Versuche: _____

Wie bist du beim Aufschreiben der Möglichkeiten vorgegangen? Wie kannst du sicher sein, dass du keine Möglichkeit doppelt aufgeschrieben hast? In der Kombinatorik (einem Teilgebiet der Mathematik) und auch in der Informatik können Baumdiagramme verwendet werden, um aufzuzeigen, welche und wie viele Möglichkeiten es gibt. Wir haben einen vierstelligen PIN-Code gesucht. Mit Hilfe eines Baumdiagramms hätten die Möglichkeiten wie folgt systematisch aufgeschrieben werden können:



Aufgabe 14

Wäre es sicherer, wenn anstelle von 4 Ziffern 4 Buchstaben verwendet werden könnten? Begründe deine Antwort.

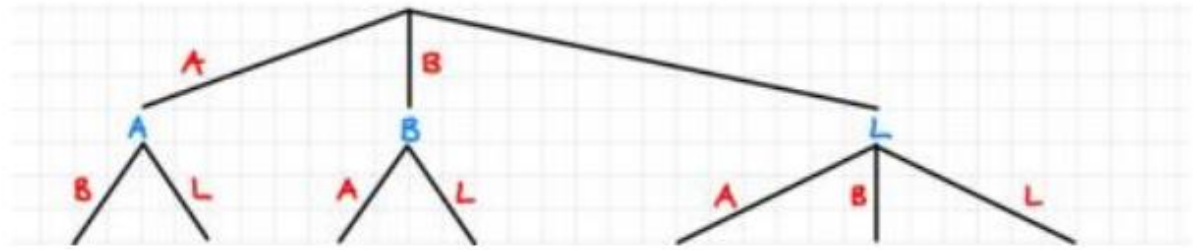
_____

_____

_____

Aufgabe 15

Welche Passwörter sind denkbar, wenn jemand ein Passwort aus vier Buchstaben zum Schutz seines Smartphones verwenden würde und das Wort aus den Buchstaben A, B, L und L besteht? Versuche die Möglichkeiten mit Hilfe eines Baumes aufzuschreiben. Vervollständige dazu das Baumdiagramm:



Fazit

Du hast gesehen, wie einfach es sein kann, ein Smartphone zu entsperren, wenn es nicht richtig geschützt wird oder ein einfaches Passwort verwendet wird. So ist es für Aussenstehende leider oft einfach, sich Zugang zu verschaffen. Also achte darauf, dass du einen Code wählst, der nicht einfach zu knacken ist!

Lösungen

Aufgabe 1
Die Computer erobern die Welt

Aufgabe 2
Individuelle Lösungen

Aufgabe 3
Individuelle Lösungen

Aufgabe 4
Die Geheimschrift zu entziffern macht Spass.

Aufgabe 5
HFJXFW

Aufgabe 6
ENABLQXKNWNKDLQBCJKNW
Differenzierungsaufgabe: ENABLQXKNWNKDLQBCJKNW

Aufgabe 7
IFXNXYJNSJAJWXHMQZJXXJQYJSFHMWNHMY
Das ist eine verschlüsselte Nachricht

Differenzierungsaufgabe:
ROGWGHSWBSJSFGQVZISGGSZHSBOQVFWQVHRWSRISBHGQVZISGGSZHVOGH
Das ist eine verschlüsselte Nachricht die du entschlüsselt hast.

Aufgabe 8
Schlüssel 7
Differenzierungsaufgabe: Schlüssel 13

Aufgabe 9
Individuelle Lösungen

Aufgabe 10
LSPWSOMPKWLEW

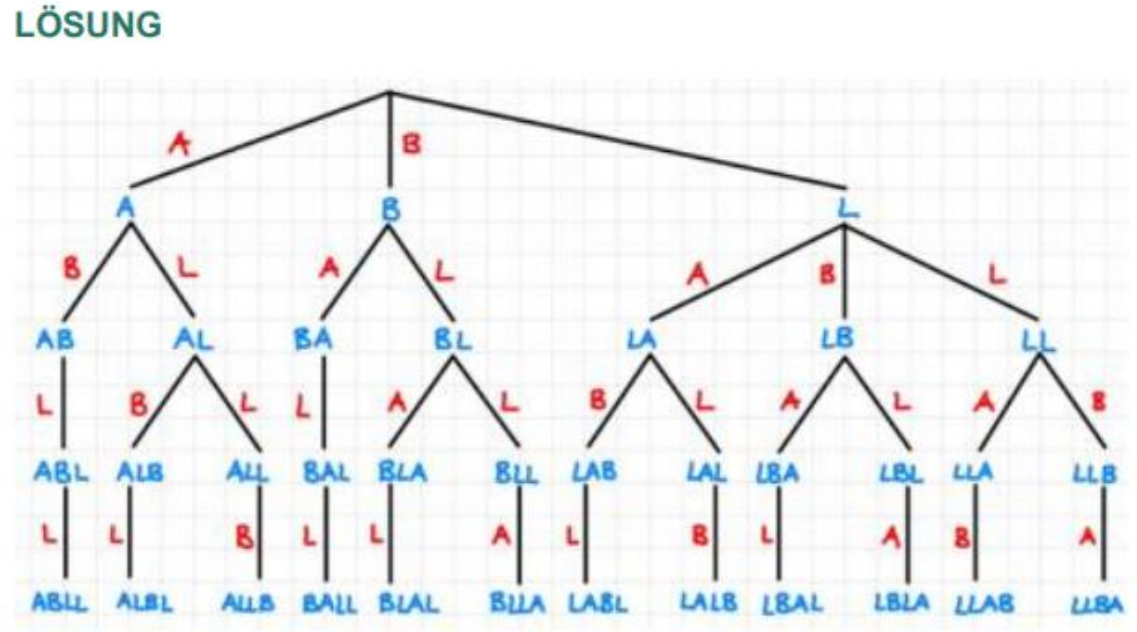
Aufgabe 11
Individuelle Lösungen

Aufgabe 12
6 Möglichkeiten
6234, 6243, 6342, 6342, 6423, 6432

Aufgabe 13
6342 (von Lehrperson bestimmt)

Aufgabe 14
Individuelle Lösungen

Aufgabe 15



Literaturverzeichnis

Einführung in die Kryptologie*, Karin Freiermuth, Juraj Hromkovic, Lucia Keller, Björn Steffen*
Einfach Informatik, Daten dartellen, verschlüsseln, kompromieren, *Juraj Hromkovic*
https://mint-erleben.lu.ch/Zyklus3/show/Information_Kommunikation

https://www.youtube.com/watch?v=4y4nCG8631g