Cäsars Rad

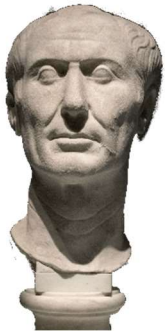
K 3

Aufgabe:

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

Übe mit den einfachen Aufgaben unten und versuche dann, eine eigene Botschaft zu verschlüsseln und mit dem Partner zu tauschen. Entschlüssle dann die Nachricht deines Partners.

Zeit: 30‘ **Sozialform:** PA



Der römische Feldherr Julius Caesar (100 bis 44 v.Chr.) verschlüsselte seine geheimen Nachrichten, indem er jeden Buchstaben durch einen anderen ersetzte. Dabei wurde der Buchstabe immer durch den um eine bestimmte Anzahl von Stellen im Alphabet verschobenen Buchstaben ersetzt. Diese Anzahl der Stellen heißt Caesar-Schlüssel.

Beim Schlüssel **3** nahm Caesar immer den Buchstaben, der im Alphabet drei Stellen weiter rechts steht. Dazu schrieb er das Alphabet zweimal untereinander. Das untere Alphabet schrieb er allerdings um drei Stellen verschoben.

Klartext

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

Verschlüsselung

Caesar ersetzte also in seinem Text jedes A durch ein D, jedes B durch ein E usw. Beachte, dass X durch A ersetzt wird, also das Alphabet nach dem Z einfach mit A weitergeschrieben wird.

Damit nicht jedes Mal die beiden gegeneinander verschobenen Alphabete aufgeschrieben werden müssen, kann auch eine sogenannte Chiffrierscheibe benutzt werden. In der Abbildung ist wie im Beispiel der Schlüssel **13** eingestellt. Mit der Scheibe kannst du nun sowohl Texte verschlüsseln als auch entschlüsseln. Möchtest du verschlüsseln, dann suchst du den Buchstaben auf der inneren Scheibe und schreibst den entsprechenden Buchstaben auf der äußeren Scheibe auf. Entschlüsseln geht entsprechend umgekehrt: Hier suchst du den Buchstaben aussen und schreibst den entsprechenden Buchstaben auf der inneren Scheibe auf.

Verschlüsseln

Stelle den Cäsarcode mit der inneren Scheibe ein. Nimm den Klartext und schaue jeden Buchstaben auf der inneren Scheibe nach. Auf der äusseren Scheibe steht der entsprechende Geheimtext.

Entschlüsseln

Stelle den Cäsarcode mit der inneren Scheibe ein. Nimm den Geheimtext und schaue jeden Buchstaben auf der äusseren Scheibe nach. Auf der inneren Scheibe steht der entsprechende Klartext.

Die »normale« Caesar-Verschlüsselung ist ziemlich leicht zu »knacken«. Etwas schwieriger wird es, wenn das Verfahren mit einem Schlüsselwort kombiniert wird. Diese Verschlüsselung funktioniert so:

- Sender und Empfänger einigen sich auf ein Schlüsselwort.
- Dieses Wort schreibst du unter ein normales Alphabet. Buchstaben, die doppelt vorkommen, lässt du dabei weg.
- Anschliessend wird das Alphabet mit den noch nicht benutzten Buchstaben, in alphabetischer Reihenfolge beim letzten Buchstaben des Schlüsselworts beginnend, aufgefüllt. **Kein Buchstabe darf doppelt vorkommen.**

Beispiel

Schlüsselwort: GEHEIMSCHRIFT. Dieses Schlüsselwort wird unter das Alphabet geschrieben, doppelte Buchstaben werden dabei weggelassen.

Klartext

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
G	E	H	I	M	S	C	R	F	T																

Verschlüsselung

Nun wird mit den restlichen Buchstaben aufgefüllt.

Klartext

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

Verschlüsselung

Mit dieser Tabelle wird dann ver- und entschlüsselt.

Auftrag

1) Könnt ihr die Nachricht Cäsars ohne bekannten Schlüssel entschlüsseln? **YHQL YLGL YLFL**

2) Entschlüsselt mit der Chiffrierscheibe die folgenden Nachrichten. Mögliche Schlüssel sind: 2, 7, 10, 13. Einer ist jeweils der richtige Schlüssel. Das heisst, dass man bei Verschiebung um diese Zahl die Nachricht erhält.
   a) **SPLIL RSLVWHAYH, AYLMMLU DPY BUZ ILP KLU WFYHTPKLU**?
   b) **YVRORE PNRFNE, VPU JREQR QN FRVA**.

3) Warum ist dieses Verschlüsselungsverfahren leicht zu »knacken«?

4) Verschlüsselt und entschlüsselt gegenseitig den Titel eures Lieblingsbuches mit dem Schlüsselwort LESERATTE.

Klartext

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

Verschlüsselung

5) Entschlüssele die folgende Nachricht. Das Schüsselwort ist SCHATZSUCHE oder MEISTER-DETEKTIV;
   STG HIKMJU YVTDJ KVAJTG STG CMGXEMAX

Klartext

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

Verschlüsselung

Klartext

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

Verschlüsselung

6) Was ist der Vorteil bei dem Schlüsselwort-Caesar-Verfahren?

7) Fällt dir eine Möglichkeit ein, wie du einen Text entschlüsseln kannst, ohne alle Schlüssel durchzuprobieren? Tipp: Nutze dabei eine bestimmte Eigenschaft einer Sprache (z.B. Deutsch) aus.