

Die Cäsar-Verschlüsselung

Julius Cäsar war ein bekannter römischer Feldherr und Politiker. Er hat seine Briefe an Freunde oder Verbündete oft verschlüsselt, damit kein anderer die Nachrichten lesen konnte.

In seiner Verschlüsselung hat er jeden Buchstaben seiner Nachricht durch einen Buchstaben ersetzt, der drei Stellen später im Alphabet kommt. Aus dem Buchstaben A wurde D und aus dem Buchstaben B wurde E und so weiter.

Der Schlüssel sah so aus: Oben ist das Alphabet, man nennt es Klaralphabet. In der unteren Reihe ist das Geheimalphabet.



Nicolas Coustou - Julius Caesar

Klaralphabet																									
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
Geheimalphabet																									

Will man nun eine Nachricht verschlüsseln, ersetzt man einfach den Buchstaben des Klaralphabets durch den Buchstaben des Geheimalphabets. Probiere es einmal aus:

1. Schreibe deinen Namen auf und verschlüssele ihn mit der Cäsar-Verschlüsselung.
2. Kannst du die folgende Nachricht auch entschlüsseln?

XP GUHL LP NLQR

In diesem Beispiel wurden die Buchstaben um drei Stellen verschoben. man kann natürlich auch fünf oder acht Stellen wählen. Damit man nicht jedes Mal eine neue Tabelle anlegen muss, kann man eine so genannte Chiffrier-Maschine bauen.

Abbildung: N.Coustou - Julius Caesar. Quelle: (Public Domain)
https://commons.wikimedia.org/wiki/File:Julius_Caesar_Coustou_Louvre.png [17.11.2015]

Aufgaben

1. Verschlüssele folgenden Satz mit einer Verschiebung um vier Stellen:

„Wir treffen uns um vier Uhr vor der Schule“

W	I	R		T	R	E	F	F	E	N		U	N	S		U	M

V	I	E	R		V	O	R		D	E	R		S	C	H	U	L	E

2. Entschlüssele den folgenden Satz mit einer Verschiebung um neun Stellen:

VXAPNW PRKC NB BYJPQNCCR IDV VRCCJPNBBNW

V	X	A	P	N	W		P	R	K	C	

N	B		B	Y	J	P	N	C	C	Q	R

I	D	V		V	R	C	C	J	P	N	B	B	N	W

3. Überlege dir nun eine eigene Botschaft, die du für deinen Nachbarn oder deine Nachbarin verschlüsselst. Denke aber daran, dass du die Verschiebung deinem Nachbarn oder deiner Nachbarin auch übermitteln musst.