Die Cäsar-Verschlüsselung

Abbildung: Nicolas Coustou - Julius Caesar

Der Versuch Schriften geheim zu halten ist wahrscheinlich so alt wie das Schreiben selbst. Viele Anlässe bewegten Menschen dazu besondere Geheimsprachen zu entwickeln – etwa Krieg, diplomatische Gründe oder die Liebe.

Die Wissenschaft, die sich mit dieser Thematik beschäftigt, nennt man **Kryptologie**.

Krypto = geheim **logos** = Wort/Rede, Sinn
(-**logie** bezeichnet die Wissenschaft eines Faches)

Auch der Feldherr und Politiker Julius Cäsar (100 bis 44 v. Chr.) hat sich seinerzeit viel mit der Verschlüsselung von Nachrichten befasst. In seiner Verschlüsslung hat er jeden Buchstaben einer Nachricht durch den 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.

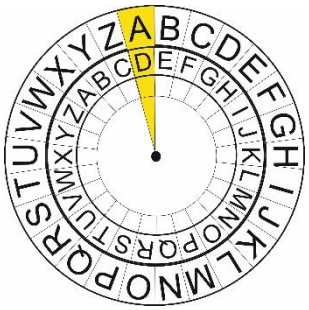
Der Schlüssel sah folgendermaßen aus. In der oberen Reihe ist das Alphabet – man nennt es Klaralphabet. In der unteren Reihe ist das Geheimalphabet.

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



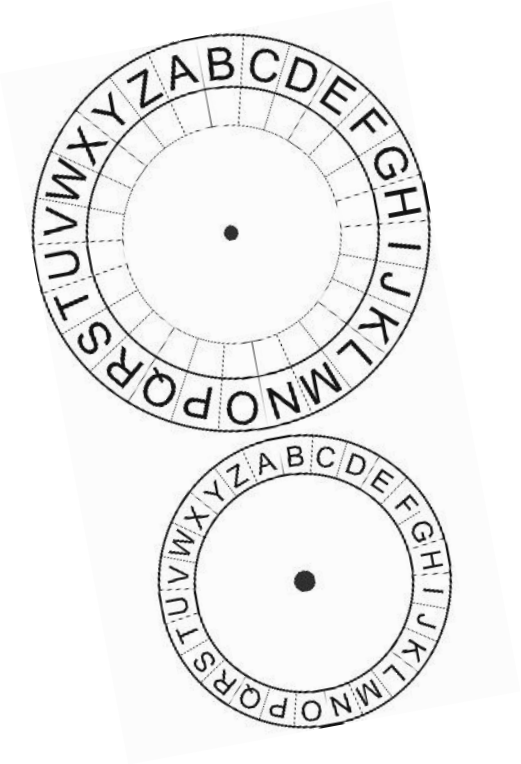
In diesem Beispiel wurden die Buchstaben um drei Stellen verschoben. Man kann natürlich auch fünf oder acht Stellen wählen. Damit man nicht jedes Mal eine neue Tabelle anlegen muss, kann man eine so genannte Chiffrier-Maschine bauen.

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

Bauanleitung

Um eine Verschlüsselungs-Scheibe zu basteln, benötigst du:

- Dünne Pappe
- Zirkel und Geodreieck
- Schere
- Kleber
- Musterklammer (benutzt man eigentlich zum Verschließen von Versandtaschen)
- Bleistift, Filzstift



1. Zeichne mit einem Zirkel zwei große Kreise nebeneinander auf eine Pappe. Ein Kreis, sollte einen Durchmesser von etwa 14 cm haben, der andere etwa 10 cm.
2. Schneide beide Kreise aus.
3. Nun müssen beide Kreise in 26 Felder unterteilt werden. Dafür ermittelst du mit Hilfe eines Geodreiecks erst einmal den Mittelpunkt. Mit dem Bleistift kannst du den Mittelpunkt aufmalen.
4. Im nächsten Schritt unterteilst du die beiden Kreise in je zwei Hälften. Der Strich muss dafür immer durch den Mittelpunkt gehen, den du gerade eingezeichnet hast.
5. Nun muss jede Hälfte in 13 Teile unterteilt werden, dafür setzt du dein Geodreieck an die Mittellinie, schiebst es um 14 Grad weiter und machst erneut einen Strich. Dies machst du, bis du alle nötigen Felder für das Alphabet hast.
6. Danach schreibst du das Alphabet in die Felder des großen und des kleinen Kreises.
7. Im letzten Schritt verbindest du beide Kreise mit der Musterklammer, fertig ist die Chiffrier-Maschine.

Übungsaufgaben

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

   „Wir treffen uns um vier Uhr vor der Schule“

   _____ _____ _____ _____ _____ _____

   _____ _____ _____ .

2. Kannst du die folgende Nachricht entschlüsseln? Die Buchstaben sind um fünf Stellen verschoben:

   BNW XHMBFJSEJS MJZYJ INJ XHMZQJ ZSI LJMJS NSX PNST

   _____ _____ _____ _____ _____

   _____ _____ _____ _____.

3. Kannst du auch eine Nachricht ohne bekannten Schlüssel knacken?

   DOOH PHLQH HQWFKHQ

   _____ _____ _____ .

4. Warum ist das Verschlüsselungsverfahren von Cäsar leicht zu knacken?

5. Welche Möglichkeiten hat man, den Schlüssel der Cäsar-Verschlüsselung herauszubekommen? Gibt es mehrere Möglichkeiten?

Wie kann man den Code knacken?

Um die Cäsar-Verschlüsselung zu dekodieren, kann man zum einen alle Möglichkeiten der Scheibe ausprobieren. Dafür benötigt man aber sehr viel Zeit.

Eine weitere Möglichkeit, um den Text zu entschlüsseln, ist zu schauen, welcher Buchstabe sehr häufig vorkommt und welche seltener vorkommen. Das liegt an den Eigenschaften einer Sprache. In der deutschen Sprache kommt der Buchstabe E am häufigsten vor und der Buchstabe Q sehr selten. Wenn also in einem Text ein Buchstabe sehr häufig vorkommt, dann ist dieser wahrscheinlich der Buchstabe E.

Probiere es einmal aus:

> QV PIUJCZO TMJBMV HEMQ IUMQAMV LQM EWTTBMV VIKP ICABZITQMV ZMQAMV.
>
> Häufigster Buchstabe: _____

Nutze nun deine Cäsar-Scheibe, um den Satz zu entschlüsseln. Drehe dafür den Buchstaben, der am häufigsten vorkommt, zum E auf der großen Scheibe.

> Entschlüsselte Nachricht:
>
> _____
>
> _____

Aufgabe

Überlege dir nun selbst eine Nachricht und gib sie **ohne Schlüssel** an deinen Nachbarn oder deine Nachbarin. Kann die Nachricht geknackt werden?

Häufigkeitsverteilung von Buchstaben in Prozent

E	17,40 %	**H**	4,76 %	**W**	1,89 %	**Y**	0,04 %
N	9,78 %	**U**	4,35 %	**F**	1,66 %	**X**	0,03 %
I	7,55 %	**L**	3,44 %	**K**	1,21 %	**Q**	0,02 %
S	7,27 %	**C**	3,06 %	**Z**	1,13 %		
R	7,00 %	**G**	3,01 %	**P**	0,79 %		
A	6,51 %	**M**	2,53 %	**V**	0,67 %		
T	6,15 %	**O**	2,51 %	**ß**	0,31 %		
D	5,08 %	**B**	1,89 %	**J**	0,27 %		