

Die Caesar-Chiffre

Information: Kennst du Asterix und Obelix? Ja?! - Dann weißt du, dass ihr großer Gegenspieler der Römer Julius Caesar ist. Dieser hat ein einfaches System erfunden, um geheime Botschaften zu verschlüsseln. Es ist nach ihm „Caesar-Chiffre“ benannt worden. Damit kannst du deine eigenen geheimen Botschaften verschlüsseln!!!



Und so geht's:

Schritt	Anweisung	Erfolg
1 - Das System	Die Beilage erklärt dir, wie die Caesar-Chiffre funktioniert.	
2 - Wörter entschlüsseln	Entschlüsse nun einige der Wörter auf der Beilage.	
3 - Wörter verschlüsseln	Verschlüsse einige der Wörter.	
4 - Geheime Botschaften	Verfasse deine eigene geheime Botschaft.	
5 - So arbeiten Kryptologen	So kann man Codes zu knacken!	

Die Caesar-Chiffre

Beilage 2:

Schritt 1

Die **Caesar-Chiffre** ist ein einfaches Verschlüsselungssystem. Sie funktioniert mit einer Buchstabenverschiebung. Man schreibt das Klartextalphabet und darunter um beliebige Stellen, z.B. zwei, „verschoben“ das verschlüsselte Alphabet. Statt des „normalen“ Klartextbuchstaben verwendet man in der chiffrierten Nachricht nun den darunter stehenden und erhält so eine verschlüsselte Botschaft. Zum Entschlüsseln muss der Empfänger natürlich den Code, in diesem Fall „2“, haben und wissen, dass eine Caesar-Chiffre verwendet wurde.

Beispiel für Caesar-Chiffre: Die erste Zeile ist das Klartextalphabet, darunter das um zwei Stellen verschobene.

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
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

Bei dem Verschlüsseln einer Nachricht wird aus einem C nun ein A, aus einem E ein C, aus einem F ein D, usw. So wird aus Haus beispielsweise: **FYSQ**.
Oder aus Tag - **RYE**.

Schritt 2: Verstanden?? - Gut! Nun kannst du die verschlüsselten Wörter entschlüsseln:

RGCP KYSQ FSLB AMKSRCP

Schritt 3 Verschlüsseln - Die Wörter dürfen keinesfalls verstanden werden! Verschlüsse sie mit Hilfe der obigen Caesar-Chiffre.

GEHEIM ABEND FENSTER BRIEF

Schritt 4: Geheime Botschaften - Nun kannst du deine eigenen Nachrichten verschlüsseln. Wähle dafür eine beliebige Verschiebung des Alphabetes.

Und wie du geheime Botschaften entschlüsseln kannst, erfährst die auf der nächsten Seite.

Die Caesar-Chiffre

Beilage 2:

Schritt 5: So kannst arbeiten Kryptologen: Versuche fremde Codes zu knacken.

Kryptologen sind Menschen, die sich mit dem Verschlüsseln und Entschlüsseln von Geheimbotschaften beschäftigen.

Und so kann man eine Caesar-Chiffre knacken, auch wenn man den Schlüssel nicht kennt: Die Buchstaben sind im Deutschen ungleichmäßig verteilt. Manche kommen öfter vor als andere, am häufigsten das „e“, gefolgt vom „n“. Danach kommen „i“, „r“, „s“, „a“ und „t“, die in etwa gleich oft vorkommen. Bei einer genügend langen Nachricht, kann mit diesen Informationen und ein bißchen Raten die Botschaft entschlüsseln.

BZAVCM: YZM IVXCWVM DNO YZM NXCPGYDBZ

Z kommt viermal vor. Wir vermuten, dass es sich um ein ein handelt.

Die Buchstabenkombination YZM gibt es zweimal. Eine Möglichkeit wäre, dass es sich um das Wort DER handelt, dann wäre das M ein R, und das Y ein D.

BZAVCM: YZM IVXCWVM DNO YZM NXCPGYDBZ
E R: DER R DER D E

Und jetzt musst du ein bisschen probieren: D kommt zweimal vor, es könnte z.B. ein I sein, N ist vielleicht ein S,

Kannst du die Nachricht entschlüsseln?