VERSCHLÜSSELUNG

In der Informatik ist die Verschlüsselung sehr wichtig, **um private Informationen geheim zu halten**. Bei der Verschlüsselung wird eine Nachricht nach einem bestimmten Verfahren (Algorithmus) **verschlüsselt**. Der **Nachrichtenempfänger** besitzt den **Schlüssel**, um die Nachricht zu **entschlüsseln**. Eine Person von Außerhalb kann die Nachricht nicht entschlüsseln, wenn sie den Schlüssel nicht weiß. Damit wissen nur Schlüsselbesitzer über den Inhalt der Nachricht Bescheid.

Es gibt viele **verschiedene Verschlüsselungsarten**. Manche kann man **schnell entschlüsseln**, auch wenn man den Schlüssel nicht besitzt. Das ist bei der Caesar-Verschlüsselung der Fall. Manche Verfahren sind so kompliziert, dass sie **niemand entschlüsseln** kann, der den Schlüssel nicht besitzt (zu viele Schlüsselmöglichkeiten).

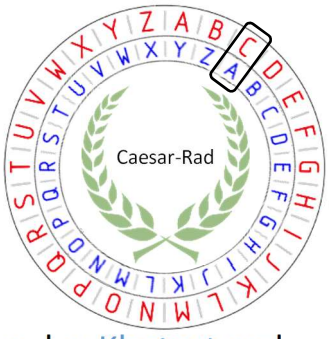
CÄSAR-VERSCHLÜSSELUNG

Bei der Caesar-Verschlüsselung werden die Buchstaben unseres Alphabets verwendet. Man **verschiebt die Buchstaben um eine gewisse Anzahl** nach rechts oder links und bekommt so den verschlüsselten Buchstaben heraus. Der **geheime Schlüssel** gibt an, um **wie viele Stellen** die Buchstaben verschoben werden.

Dazu schreibt man das Alphabet zweimal untereinander. Das untere Alphabet wird in unserem Beispiel um **zwei Stellen nach rechts** verschoben:

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

Die **blauen** Buchstaben sind der **KLARTEXT**, die **roten** Buchstaben sind der **VERSCHLÜSSELTE TEXT**.



Beispiele:

KINDER → MKPFGT

FCU KUV IGJGKO → DAS IST GEHEIM

Verschlüsseln und Entschlüsseln mit dem Caesar-Rad:

Stelle den Cäsar-Code (1-25) 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.