

Station A: Die Cäsar-Verschlüsselung

Diese Verschlüsselungsmethode soll der römische Kaiser Gaius Julius Cäsar als erster verwendet haben. Deshalb ist das folgende Verfahren nach ihm benannt.

Die klassische Cäsar-Verschlüsselung ersetzt in jedem Buchstaben des Klartextes durch den im Alphabet drei Stellen weiter hinten liegenden. Es wird also a durch D, b durch E, usw... ersetzt. Die letzten drei Buchstaben x, y und z werden durch A, B und C verschlüsselt. Die einzelnen Ersetzungen sind in folgender Tabelle zusammengefasst.

Klar	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
Geheim	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

Da man die zu verschlüsselnden Buchstaben an der gleichen Stelle belässt und sie durch einen anderen Buchstaben ersetzt, ist das Cäsar-Verfahren ein Beispiel für eine **Substitutionschiffre** (von lat. *substituere* = ersetzen).

Beispiel 1 (Verschlüsselung): Der Klartext: ich kam, sah und siegte. Wir ersetzen jeden Buchstaben nach obiger Tabelle und erhalten als Geheimtext: LFK NDP, VDK XQG VLHJWH.

Beispiel 2 (Entschlüsselung): Der Geheimtext lautet: JDQC JDOOLHQ LVW EHV LHJW. Wir lesen in der obigen Tabelle "von unten nach oben" und erhalten als Klartext: ganz gallien ist besiegt.

Aufgabe 1:

- Verschlüssele den Klartext `razzia`. Entschlüssele den Geheimtext `FDHVDU`.
- Natürlich kann man auch um eine andere Stellenzahl als 3 verschieben. Die Zahl ist dann der Schlüssel des Verfahrens.
Verschlüssele nun den Klartext `informatik` mit dem Schlüssel 13. Entschlüssele den Geheimtext `UFVYLN YCHMNYCH` mit dem Schlüssel 20.

Aufgabe 2: Wie viele verschiedene Schlüssel gibt es für dieses Verfahren?

Aufgabe 3 (Zusatz): Entschlüssele den Geheimtext `GYZKXOD ATJ UHKROD`. Wie lautet der Schlüssel? Beschreibe deine Vorgehensweise.