Die Geschichte der Cäsar-Verschlüsselung

Die **Verschiebechiffre** (auch als **Cäsar-Verschlüsselung** oder schlicht als **„Einfacher Cäsar"** bezeichnet) ist ein besonders einfacher Sonderfall einer simplen monoalphabetischen Substitution. Zum Zwecke der Verschlüsselung wird dabei jeder Buchstabe des lateinischen Standardalphabets um eine bestimmte Anzahl von Positionen zyklisch verschoben (rotiert). Die Anzahl bestimmt den Schlüssel, der für die gesamte Verschlüsselung unverändert bleibt. Es ist eine der einfachsten und sichersten Formen einer Geheimschrift.
Der Name der Cäsar-Verschlüsselung leitet sich vom römischen Feldherrn Gaius Julius Cäsar ab, der diese Art der geheimen Kommunikation für seine militärische Korrespondenz verwendete. Dabei benutzte Cäsar selbst häufig den Schlüssel C, also eine Verschiebung des Alphabets um drei Buchstaben. Der römische Kaiser Augustus soll eine Verschiebung der Buchstaben um nur eine Position vorgezogen haben (vielleicht passend zu seinem Namen, der mit A beginnt).

Gaius Julius Cäsar
(* 100 v. Chr. † 44 v. Chr.)

Der römische Schriftsteller Sueton beschreibt das Verfahren wie folgt:
„… si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet."
„… wenn etwas Geheimes zu überbringen war, schrieb er in Zeichen, das heißt, er ordnete die Buchstaben so, dass kein Wort gelesen werden konnte. Um diese zu lesen, tauscht man den vierten Buchstaben, also D, gegen A aus und ebenso mit den restlichen."

Die Cäsarchiffre wird als Teil komplexerer Verschlüsselungsverfahren – etwa der 1508 von Trithemius zum ersten mal mit Hilfe seiner Tabula recta erläuterten polyalphabetischen Substitution oder auch der Vigenère-Chiffre – eingesetzt. Selbst heute noch ist sie in Gestalt des in der elektronischen Kommunikation verbreiteten ROT13-Systems zur Verschleierung von Nachrichten in Gebrauch. (Quelle: Wikipedia)

Cäsars Geheimnis

Aus Cäsars Zeit ist ein Text erhalten geblieben. Leider ist der Text verschlüsselt.
Versuche, den Text zu entschlüsseln und – wenn Du willst - die gestellte Aufgabe zu lösen.
(Für die Verschlüsselung wurde ein Verschiebefaktor von 6 gewählt!)

KOTKS WAGJXGZ GHIJ OYZ KOT XKINZKIQ SOZ JKT YKOZKTRGKTMKT 10 IS ATJ 4 IS KOTHKYINXOKHKT.
HKXKINTK JKT LRGKINKTOTNGRZ JKY WAGJXGZKY!

Nutze die unten aufgeführte Tabelle und entschlüssele Buchstabe für Buchstabe, bis Du den ganzen Text lesen kannst!

K	O	T	K	S		W	A	G	J	X	G	Z		G	H	I	J		O	Y	Z		K	O	T
E	**I**	**N**	**E**	**M**																					

X	K	I	N	Z	K	I	Q		S	O	Z		J	K	T		Y	K	O	Z	K	T	R	G	K

T	M	K	T		1	0	I	S		A	T	J		4	I	S		K	O	T	H	K	Y	I	N

X	O	K	H	K	T	.		H	K	X	K	I	N	T	K		J	K	T		L	R	G	K	I

N	K	T	O	T	N	G	R	Z		J	K	Y		W	A	G	J	X	G	Z	K	Y	!		