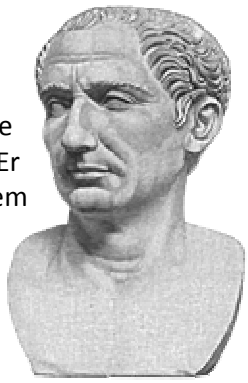
Das Geheimnis des römischen Kaisers Caesar



Der römische Feldherr und Kaiser Gaius Julius Caesar (100 – 44 v. Chr.) verschlüsselte angeblich seine geheimen militärischen Botschaften nach folgendem Verfahren: Er verwendete ein Geheimtextalphabet (GTA), welches um drei Stellen gegenüber dem Klartextalphabet (KTA) verschoben war. Jeder Buchstabe des Klartextes wurde durch einen Buchstaben aus dem Geheimtextalphabet ersetzt:

Klartext: E IN STRENG GEHEIMER TEXT

KTA	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	Y	Z	A
GTA	C	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	D

Geheimtext: HLQVWUHQJJHKHLPHUWHAW

Vermutlich verwendete Caesar die Verschiebung um genau drei Stellen, weil sein Name mit dem dritten Buchstaben des Alphabetes - dem C - begann. Kaiser Augustus (31 v. Chr. - 14 n. Chr.) soll dagegen die Verschiebung um eine Stelle bevorzugt haben. Zur höheren Sicherheit verwendet man nur Großbuchstaben, keine Umlaute und lässt Leerzeichen, Satzzeichen usw. weg.

Um einen Text zu verschlüsseln, legt man 2 Doppelstreifen übereinander und verschiebt den unteren Streifen entsprechend (siehe Abbildung oben). So lässt sich für jedes Zeichen des Klartexts das entsprechende Zeichen des Geheimtextalphabets auf dem unteren Streifen ablesen.

Zum Entschlüsseln suche den Buchstaben auf dem unteren Streifen und lese den Buchstaben des Klartexts auf dem oberen Streifen ab.

Aufgaben

1. Tausche mit einem Partner kleine Geheimnisse per E-Mail aus. Damit niemand außer euch beiden die Geheimnisse erfährt, solltet ihr die E-Mails nach dem Cäser-Verfahren verschlüsseln. Gehe dabei wie folgt vor:
   a. Vereinbare zu allererst mit deinem Partner, um wie viele Buchstaben ihr die Alphabete verschieben wollt (→ „Abstand zwischen KTA und GTA“)!
   b. Denke dir ein kleines Geheimnis aus und schreibe es in einem kurzen Satz auf!
   c. Verschlüssle den Satz mit Hilfe der Albertischeibe und sende den verschlüsselten Satz deinem Partner in einer E-Mail.
   d. Entschlüssle das Geheimnis deines Partners, das er dir in einer E-Mail geschickt hat, mit Hilfe der Albertischeibe!
2. *Georg der Gangster* hat im Internet folgende vermutlich mit dem Caesar-Verfahren verschlüsselte Nachricht abgefangen: MGLRYXDIGEIWEV
   a. Versuche, den Code auch ohne Kenntnis des Abstands zwischen KTA und GTA zu knacken! *Hinweis:* Probiere doch einfach mal ein paar Abstände mit einem Teil der Nachricht aus!
   b. Wie sicher ist die Verschlüsselung nach dem Caesar-Verfahren? Begründe deine Antwort! *Hinweis:* Wie viele verschiedene Geheimtextalphabete gibt es mit diesem Verfahren?
3. Knobelaufgabe für Schnelle: Angenommen, die Buchstaben des Geheimtextalphabets werden in beliebiger Reihenfolge zugeordnet, z.B. folgendermaßen:

KTA	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
GTA	G	Q	H	C	D	U	K	O	X	A	L	P	F	S	J	B	T	Z	R	I	E	N	V	Y	W	M

   Wie würde sich diese Veränderung auf die Sicherheit der Verschlüsselung auswirken? *Hinweis:* Wie viele verschiedene Geheimtextalphabete kann es bei diesem Verfahren geben?