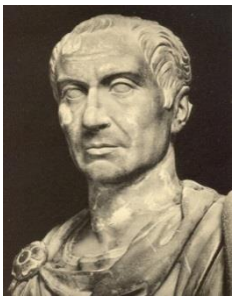
Arbeitsauftrag Informatik
Name: **Vorname:** **Klasse:**

Die Geheimsprache von Julius Caesar



GAIUS JULIUS CAESAR (*100 v. Chr.; † 44 v. Chr.) war ein römischer Staatsmann, Feldherr und Autor. Nach Überlieferung des römischen Schriftstellers SUETON übermittelte CAESAR seine militärische Korrespondenz stets verschlüsselt. Aus heutiger Sicht ist das klassische Caesar-Verfahren zwar primitiv, gilt aber als der Urvater aller Verfahren, bei dem die Zeichen des Klartextes durch andere Zeichen oder Symbole ausgetauscht werden. Solche Verfahren bezeichnet man als **Substitutionsverfahren**.

CAESAR ersetzte jeden Buchstaben im Klartext durch einen Buchstaben, der (zyklisch) 3 Stellen weiter hinten im Alphabet stand, also mit dem Schlüssel `a` → `D`:

Geheimtextalphabet: **D**EFGHIJKLMNOPQRSTUVWXYZABC
Klartextalphabet: **a**bcdefghijklmnopqrstuvwxyz

1) Zeige, dass `HALLO` zu `KDOOR` wird.
2) Entschlüssle CAESARS Ausspruch: `LFK NDP, VDK XQG VLHJWH`.
3) Verschlüssle mit Hilfe der Caesar-Scheibe und mit dem Schlüssel `T` den lateinischen Caesar-Spruch: „`lacta alea est`“.
4) Versuche die Nachricht `SQUIQH MQH ISXBQK` ohne Kenntnis des Schlüssels zu bestimmen.

CAESAR mit Schlüsselwort

Zum Brechen des CAESAR-Verfahrens mit variablem Schlüsselbuchstaben muss man nur 25 Möglichkeiten ausprobieren. Eine komplexere Anordnung des Geheimtextalphabets erhält man mit Hilfe eines Schlüsselwortes und eines Startbuchstabens.

Geheimtextalphabet: WYZ**ASTERIX**BCDFGHJKLMNOPQUV
Klartextalphabet: abc**d**efghijklmnopqrstuvwxyz

5) Entschlüssle `EWFV EWCCISF` mit dem gegebenen Geheimtextalphabet.
6) Verschlüssle die Nachricht `Das ist doch sicher` mit dem Schlüsselwort `INFORMATIK` und dem Buchstaben `Q`.
7) Werden die Buchstaben so durcheinander gewürfelt, ergeben sich für einen Angreifer 26·25·24·…·3·2·1 - 1 = 403291461126605635583999999 Varianten. Diese können von modernen Rechnern nicht in einer vernünftigen Zeit durchprobiert werden, selbst bei bis zu 350 Millionen Versuche pro Sekunde! Zum Brechen der Verschlüsselung müssen statistische Methoden eingesetzt werden. Wie lange würde es denn dauern?