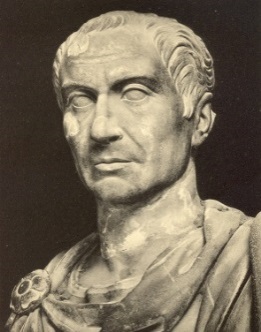
# Die Geheimsprache von Julius Caesar

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. Er gilt als Begründer der klassischen Kryptologie. Aus heutiger Sicht ist das Caesar-Verfahren zwar primitiv, ist aber der Urvater aller Verfahren, bei die Zeichen des Klartextes durch andere Zeichen oder Symbole ausgetauscht werden. Solche Verfahren bezeichnet man als **Substitutionsverfahren**.

Caesar ersetzte jeden Buchstaben im Klartext mit einem Buchstaben, der 3 Stellen zyklisch weiter hinten im Alphabet steht, also mit dem Schlüssel A 🡪 D:

Geheimtextalphabet: **D**EFGHIJKLMNOPQRSTUVWXYZABC

Klartextalphabet: **A**BCDEFGHIJKLMNOPQRSTUVWXYZ

1. Entschlüssle Caesars Ausspruch: LFK NDP, VDK XQG VLHJWH.
2. Verschlüssle mit Hilfe der Caesar-Scheibe und mit dem Schlüssel T den lateinischen Caesar-Spruch: „Lacta alea est“.
3. 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 probieren. Eine bessere Anordnung des Geheimalphabets erhält man mit Hilfe eines Schlüsselwortes und Startbuchstaben.

Geheimtextalphabet: WYZ**ASTERIX**BCDFGHJKLMNOPQUV

Klartextalphabet: ABC**D**EFGHIJKLMNOPQRSTUVWXYZ

Werden die Buchstaben so durcheinander gewürfelt, ergeben sich für einen Angreifer 26·25·24·…·3·2·1 - 1 = 403291461126605635583999999 Varianten. Diese können selbst von modernen Rechnern nicht in einer vernünftigen Zeit durchprobiert werden, selbst wenn sie bis zu 350 Millionen Versuche pro Sekunde schaffen. Zum Brechen der Verschlüsselung müssen statistische Methoden eingesetzt werden.

1. Entschlüssle EWFV EWCCISF.
2. Berechne die maximale Zeit für das Finden des korrekten Geheimtextalphabets mit 26 Buchstaben bei einem unbekannten Substitutionsverfahren.

## Lösung

1. Ich kam sah und siegte
2. ETVMT TEXT XLM
3. CAESAR WAR SCHLAU (Schlüssel Q)
4. GANZ GALLIEN
5. 26·25·24·…·3·2·1 - 1 = 403291461126605635583999999

403291461126605635583999999 : 350000000 s-1

≈ 1,152261317·1018 s

≈ 3,653796667·1010 Jahre

Zum Vergleich: Die Erde ist ca. 4,7·109 Jahre alt.