# Die verbesserte 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:

Eine bessere Anordnung des Geheimalphabets erhält man mit Hilfe eines Schlüsselwortes und Startbuchstaben, hier im Beispiel **ASTERIX** und **D**.

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, auch wenn sie bis zu 350 Millionen Versuche pro Sekunde schaffen. Zum Brechen der Verschlüsselung müssen statistische Methoden eingesetzt werden.

1. Entschlüssle, den mit **ASTERIX** und **D** verschlüsselten Text EWFV EWCCISF.
2. Berechne die maximale Zeit für das Finden des korrekten Geheimtextalphabets mit 26 Buchstaben bei einem unbekannten Substitutionsverfahren.