# 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.