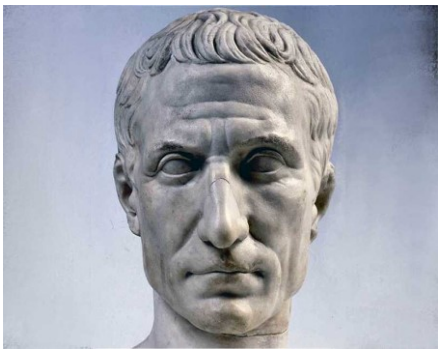
Kapitel 3: Caesar-Verschlüsselung

Die Geschichte der Kryptographie beginnt mit den symmetrischen Chiffrierverfahren, die zahlreiche Verschlüsselungsarten beinhalten, ein Verfahren möchten wir uns genauer anschauen: Die Caesar-Verschlüsselung.



Der römische Feldherr Julius Caesar (100 bis 44 v. Chr.) verschlüsselte seine gemeinem Nachrichten, indem er jeden Buchstaben durch einen anderen ersetzte (= **Substitution**). Dabei wurde der Buchstabe immer durch den um eine bestimmte Anzahl von Stellen im Alphabet verschobenen Buchstaben ersetzt. Wir nennen das Verfahren auch die **monoalphabetische Substitution**, bei der jeder Buchstabe des Klartextalphabets durch einen anderen festgelegten Buchstaben des Geheimalphabets ersetzt wird.

Variante: Die Einfache Caesar-Verschlüsselung

Bei diesem einfachen verschlüsselungsverfahren wird einfach jeder Buchstabe des Klartextalphabets durch einen, um eine festgelegte Anzahl an Stellen weiter hinten im Alphabet stehenden Buchstaben ersetzt. Die Stellenverschiebung nennt man einfach Caesar-Verschiebung.

Beispiel mit Caesar-Verschiebung **4**:

Klartextalphabet:	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
Geimtextalphabet:	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
Klartext:	Hallo, Caesar
Geheimtext:	LEPPS, GEIWEV

Praktische Anwendung

Drucke dir die Vorlage_Chiffrierscheibe aus bastle dir deine eigene Chiffrierscheibe! Du benötigst dafür die Vorlage, Kleber, Schere und eine Musterbeutelklammer.