**Die Caesar-Verschlüsselung**

Die Römer unter dem Feldherrn Julius Caesar (100 – 44 v. Chr.) wollten damals Botschaften verschicken, die nur sie entziffern konnten. Der Text wurde so verändert, dass eine auf dem ersten Blick unlesbare Buchstabenfolge entstand, welche von den Römern wieder lesbar gemacht werden konnte.

Die Caesar-Verschlüsselung benutzt folgendes Verfahren:  
Jedem Zeichen im Klartext wird ein Geheimtextbuchstabe- oder Symbol zugeordnet. In diesem Beispiel wurde im Alphabet der Buchstabe A durch D ersetzt. Die restlichen Buchstaben wurden jeweils mit den 3 Stellen weiter hinten im Alphabet befindlichen Buchstaben ersetzt.

Klartext: abcdefghijklmnopqrstuvwxyz

Geheimtext: DEFGHIJKLMNOPQRSTUVWXYZABC

1. Überprüfe mit oben genannten Schlüssel, ob die verschlüsselte Nachricht gdvlvwfdhvdu dasistcaesar ergibt.
2. Verschlüssel den Text „Gallien erobern“ mit dem oben angegebenen Schlüssel.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Entschlüssel die Nachricht „IRAV IVQV IVPV“ mit dem Schlüssel a-> N

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Nimm dir einen der Texte auf dem Tisch und entschlüssel diesen. Die Lösung befindet sich zur Selbstkontrolle auf der Rückseite. Schreibe auf einem unbeschriebenen Zettel selber eine Nachricht mit der Lösung auf der Rückseite.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Beschreibe und erkläre, warum dieses Verfahren einfach zu entschlüsseln ist!
2. Erläutere, ob das Verfahren sicherer wird, wenn dies zweimal angewendet wird?

**Caesar-Verschlüsselung mit Schlüsselwort**

Die Komplexität des Geheimtextalphabetes lässt sich durch ein Schlüsselwort erhöhen.

Geheimtextalphabet: wxyz**tagung**bcdefhijklmopqrs

Klartextalphabet: abcd**e**fghijklmnopqrstuvwxyz

1. Entschlüssel umtltznyuofjxjmlmk mithilfe des vorgegebenen Geheimtextalphabetes.
2. Verschlüssel eine selbstgewählte Nachricht mit einem ausgewählten Schlüsselwort. Beschreibe dein Vorgehen.