**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.



1. Überprüfe mit oben genannten Schlüssel, ob die verschlüsselte Nachricht gdvlvwfdhvdu DasistCaesar ergibt.

Richtig

1. Verschlüssel den Text „Gallien erobern“ mit dem oben angegebenen Schlüssel.

Jdoolhq hurehuq

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

Veni vidi vici

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.  
     
   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Beschreibe und erkläre, warum dieses Verfahren einfach zu entschlüsseln ist!

Maximal 26 Versuche.

1. Erläutere, ob das Verfahren sicherer wird, wenn dies zweimal angewendet wird?   
   Nein, denn es bleibt bei 26 Versuchen.

**Caesar-Verschlüsselung mit Schlüsselwort**

Die Komplexität des Geheimtextalphabetes lässt sich durch ein Schlüsselwort erhöhen.

Geheimtextalphabet: wxyz**tagung**bcdefhijklmopqrs

Klartextalphabet: abcd**e**fghijklmnopqrstuvwxyz

1. Entschlüssle umtltznyuofjxjmlmk mithilfe des vorgegebenen Geheimtextalphabetes.

huetedichvorbrutus

1. Verschlüssle eine selbstgewählte Nachricht mit einem ausgewählten Schlüsselwort. Beschreibe dein Vorgehen.