

# Aufgaben zur symmetrischen Verschlüsselung

**Transpositionsverfahren:** Nachrichtenteile werden umgestellt (permutiert)

Beispiel 1: Permutation mit fester Periode 4

D	E	R	S	C	H	A	T	Z	I	S	T
R	E	S	D	A	H	T	C	S	I	T	Z

Schlüssel: 3 2 4 1

Beispiel 2: Transpositionsmatrix

Schlüssel ergibt die Anzahl der Spalten

Geheimtext wird spaltenweise ausgelesen

D	E	R	S
C	H	A	T
Z	I	S	T

Schlüssel = 4  
Geheimtext = DCZEHIRASSTT

- 1) Entschlüsseln Sie die folgende Zeichenkette unter der Annahme, dass der Schlüssel = 6 ist!

IDTECEONHRRBBDEAIOIRNKST

## Cäsar-Chiffre

Verschieben des Alphabets

Beispiel: verschieben um 3 Buchstaben

Klartext: a b c d e f g h i j k l m ...

Geheimtext: D E F G H I J K L M N O P ...

**GLH VSLQQHQ GLH JDOOLHU =**

**Die spinnen die Gallier**

**2) Entschlüsseln Sie den Text mithilfe der unten stehenden Angaben!**

**cgtt qusskt cox jxko aty cokjkx ktzmkmkt  
ot juttkx ot hrozfkt ujcx ot xkmkt**

Cäsar-Chiffre mit Verschiebung um 5

**Polybius Verschlüsselung (-> Internet..)**

**3) Verschlüsseln Sie folgenden Text mit der Polybius-Methode:**

*Diese Nachricht ist ausschließlich für Dich!*

Viel Erfolg!