1. Allgemein

- Die Buchstaben der Nachricht verändern "die Gestalt" (= werden durch andere ersetzt), aber behalten ihre Position innerhalb der Nachricht
- Veränderung erfolgt durch Verknüpfung der Klartext-Nachricht mit sog. Geheimtextalphabet
- **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

2. Beispiel – Schlüssel des Caesar

- zyklische Vertauschung der Buchstaben des Alphabets (monoalphabetisch)
- dechiffrieren Sie die Buchstabenkombination **L W P D F K W V S D V V** nach Krebschlüssel Caesar 3!

Lösung: .....

3. Beispiel: Vigenère-Quadrat

- Verschlüsselungsvorschrift wechselt während der Verschlüsselung (polyalphabetisch)
- Algorithmus von Vigenère: Schlüsselwort + Vigenère-Quadrat.

	Klartext																								
	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
Schlüssel																									
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	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
E	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
F	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	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	**R**	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Geheimtext

- **Schlüsselwort:** beliebig, Länge richtet sich i.d.R. nach der Länge der Nachricht
  - Verschlüsseln Sie das Wort **K A F F E E K A N N E** nach dem Algorithmus von Vigenère!
  - Verwenden Sie als Schlüsselwort: **B I E R**

Lösung:

Geheimnis	K	A	F	F	E	E	K	A	N	N	E
Schlüsselwort	B	I	E	R	B	I	E	R	B	I	E
Chiffrat	L	I	J	W	F	M	O	R	O	V	I

Transposition

1. Allgemein

- Die Buchstaben der Nachricht werden anders angeordnet (Reihenfolge wird vertauscht)
- Anordnungsmöglichkeiten (= Permutationen) hängen von der Länge der Mitteilungen ab

2. Beispiel: Gartenzaun-Transposition

1. Beispiel: Um die Geheimbotschaft zu erstellen, werden die Buchstaben einer Mitteilung abwechselnd in zwei (mehrere) Zeilen geschrieben und dabei die Leerräume entfernt. Danach wird der Inhalt der einzelnen Zeilen hintereinander geschrieben (mit der obersten Zeile beginnend)

W	E	R		R	E	I	T	E	T		S	O		S	P	Ä	T		D	U	R	C	H		N	A	C	H	T		U	N	D		W	I	N	D
W		R			E		T			T		O			P		T			U		C			N		C		T			N			W		N	
W		R		R																																		
WRETTOPTUCNTNWN ERIESSÄDRHAHUDID																																						

2. Beispiel: Entschlüsseln Sie folgende Geheimbotschaft
(Verschlüsselung mit 2-zeiliger “Gartenzaun-Transposition”)!

		M	R	E	S	U	D	A	G	L	I	M	N	O	G	N	T	N	H	T	O	D	M	U	D		
M	O	R	G	E	N		S	T	U	N	D		H	A	T		G	O	L	D		I	M		M	U	N	D