Kryptologie

Substitution

"ein Buchstabe wird mit einem anderen ersetzt"

→ monoalphabetisch:
→ Caesar

→ polyalphabetisch
→ Vigenere

→ XOR-Chiffre

```
1101011110010 → Klartext
1010111001101 → Schlüssel
0111110111111
```

Transposition

"Reihenfolge der Buchstaben wird verändert"

A	D	C	D ...
E	F	G	H ...

	A	B	C	D ...
1	A	B	C	D ...
2	B	C	D	E ...
3	C	D	E	F ...
4	D	E	F	G ...
...	...	...	...	...

```
KLARTEXTIST
SCHLUSSELSC
.....
11
19
30 → 6
```

Kasiski-Test

1. Mehrmals vorkommende Buchstabenfolgen finden
2. Abstände bestimmen
3. ggT der Abstände bzw. andere Teiler sind Schlüssellänge
4. Schlüssel bestimmen

Symmetrisch ⟷ **Asymmetrisch**

Caesar, Vigenere, XOR

selber Schlüssel zum Ver- und Entschlüsseln

$\lceil \frac{n \cdot (n-1)}{2} \rceil$ Schlüssel für n Personen

schneller

Problem des Schlüsselaustauschs

→ Diffie-Hellmann-Algorithmus

(Potenzen u. mod)

Blockchiffre
→ Aufteilung in Blöcke
→ Verarbeitung Blockweise
→ Vertauschung der Blöcke
→ mod-Addition u. XOR

Zertifizierungsstellen

Sicherheitsziele

RSA

zwei unterschiedliche Schlüssel (öffentlicher und privater)
→ Schlüsselpaar

$\lceil 2n \rfloor$ Schlüssel für n Personen

langsamer

→ ermöglicht Signaturen
→ hashing benötigt

→ • Vertraulichkeit (keiner liest mit)
• Integrität (keiner manipuliert)
• Authentizität (Sender sicher)
• Verbindlichkeit (Sender kann nicht abstreiten)