Kryptologie I

Verschlüsselung

Substitution → **Ersetzung** eines Zeichens mit einem anderen

→ **Transposition** → **Vertauschung** der Reihenfolge der Zeichen

monoalphabetisch → Caesar

A	B	C	D	...
G	H	I	J	...

polyalphabetisch → Vigenère

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

Space ← 11 ←	K	L	A	R	T	E	X	T
Zeile → 11 ←	K	E	Y	K	E	Y	K	E
22 →	U	P	Y	B	X	.....		

XOR-Chiffre:

1	1	0	1	0	1	0	0	→ Klartext
1	0	0	1	1	0	0	1	→ Schlüssel (XOR)
0	1	0	0	1	1	0	1	→ Geheimtext

Blockchiffre: Aufteilung des Klartexts und Schlüssels in **Blöcke**; **Verkettung** der Blöcke des Klartexts und des Schlüssels in bestimmten Kombinationen über **mehrere Runden** (z.B. u. v.a. mit **XOR**) u. mod-Addition

Kryptologie II

Verschlüsselung

Symmetrisch

selber Schlüssel zum Ver- und Entschlüsseln

z.B. Caesar, Vigenere, XOR, Blockchiffre (AES)

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

schneller

→ Speicherung großer Datenmengen durch eine Person

→ Problem des Schlüsselaustausches

↓

Diffie-Hellmann-Algorithmus

(Anwendung von Potenzen und Modulo-Rechnung um einen gemeinsamen Schlüssel zu erzeugen)

Asymmetrisch

zwei unterschiedliche Schlüssel

→ Schlüsselpaar

öffentlicher / privater

z.B. RSA

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

langsamer

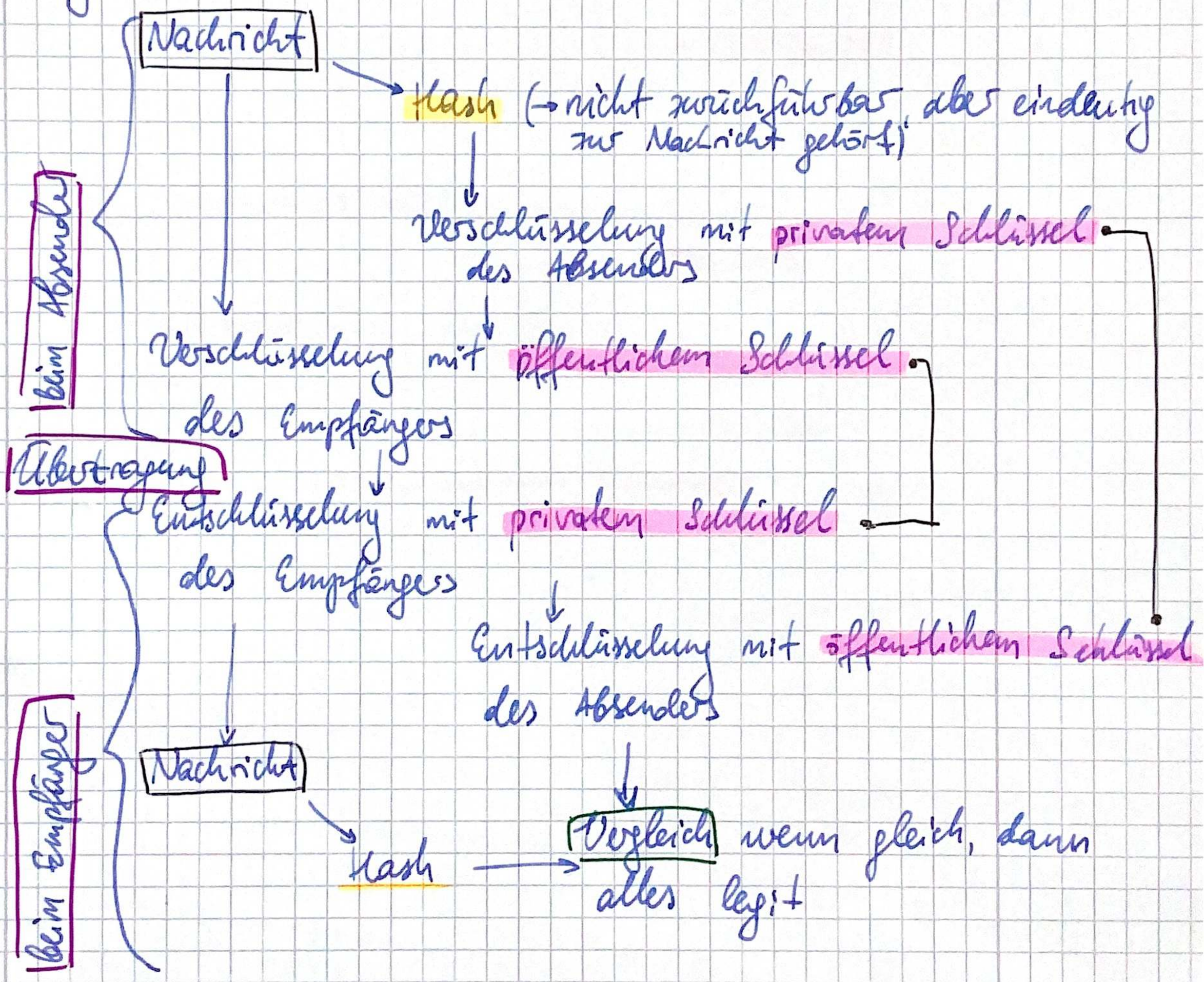
→ Kommunikation im Internet (mögliche Abhörung)

Digitale Signaturen u. Zertifikate

Sicherheitsziele
- **Vertraulichkeit** (kein Dritter liest mit)
- **Integrität** (Nachricht sicher vor Manipulation)
- **Authentizität** (sicher, wer der Sender ist)
- **Verbindlichkeit** (Sender kann Nachricht nicht abstreiten)

Beruht auf Prinzipien der **asymmetrischen Verschlüsselung**

Signatur:



Problem: wie weiß ich zu 100%, dass der öffentliche Schlüssel legit ist?

Lösung: eine vertrauenswürdige **Zertifizierungsstelle** signiert ihn

Kryptologie – Verschlüsselung Brechen

Brute-Force

- alle möglichen Schlüssel ausprobieren
- funktioniert nur bei natürlicher Sprache

Häufigkeitsanalyse

- zählen, wie oft welche Buchstabe vorkommt
  und mit Durchschnittswerten vergleichen
  (z.B. „e" häufigster)
- Sprache des Textes muss bekannt sein

Kasiski-Test

- 1. Mehrfach vorkommende Buchstabenfolgen finden
  2. Abstände bestimmen
  3. ggT der Abstände bzw. andere Teiler ist Schlüssellänge
  4. Schlüssel bestimmen
- Bricht Vigenère-Verschlüsselung