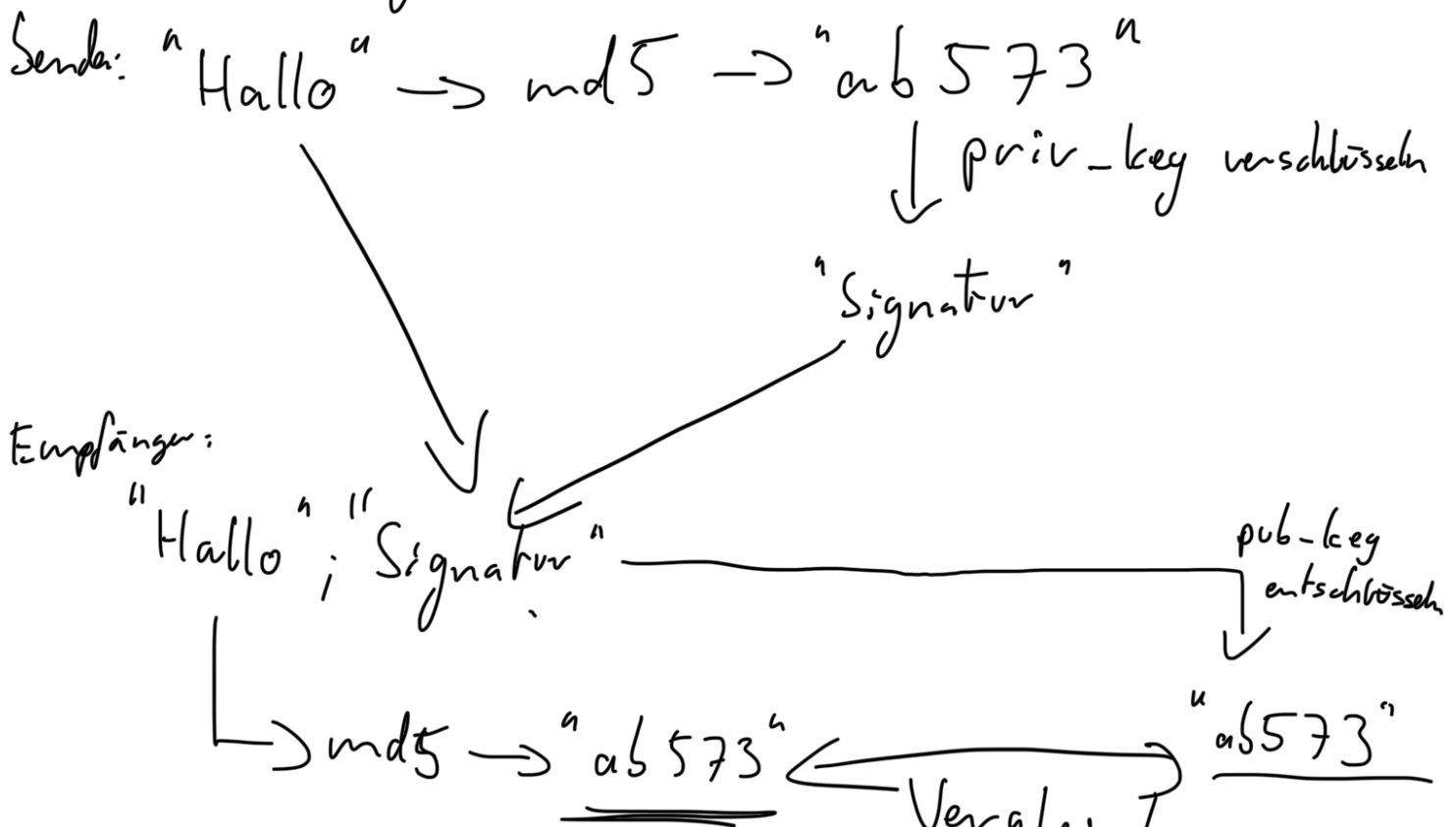


IT-Schutzziele

- Integrität: Daten nicht unbemerkt verändert
- Authentizität; Identität: Sender/Empfänger überprüfen
- Vertraulichkeit: Zugriff nur durch Sender/Empfänger
- (- Verfügbarkeit: Systeme & Daten müssen erreichbar sein)

Kryptografie

- Absicherung von Daten/Informationen durch:
- Verschlüsselung - Vertraulichkeit pub/priv
 - Hashing - Integrität
 - Signaturen - Authentizität, Integrität



gleich
✓

AES (symmetrische Verschlüsselung)

→ 1. Schlüssel zum Ver- & Entschlüsseln

Bsp.: Caesar-Verschlüsselung
Alphabetische Verschiebung:

A → D Schlüssel: 3

"Hallo Dennis"

↓
"KDOOR GHQQLV"

Nachteile:

- Häufigkeitsanalyse: E, N, S

- Mustererkennung

- begrenzter Schlüssel: $26 - 1 = 25$

Bitzahl der Schlüssellänge;

128 bit ; 192 bit ; 256 bit ; 512 bit

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

Asymmetrische Verschlüsselung (RSA)

- 2 Schlüssel: Ver- & Entschlüsseln

↳ private Key $\rightarrow$ bleibt meinen / bleibt geheim
↳ public Key $\rightarrow$ kann jeder haben

Mathematik dahinter: Primfaktorzerlegung

$$7 \times 5 = 35 \Rightarrow 7 \cdot 5$$

$$2 \cdot 7 \cdot 5 \cdot 7 \cdot 3 \cdot 15 \cdot 7 \cdot 26 \Rightarrow$$

$$p = 5; q = 11$$

$$n \Rightarrow 5 \cdot 11 = \underline{\underline{55}}$$

$$\phi(55) = (5-1) \cdot (11-1) = 4 \cdot 10 = 40$$

$$\underline{e=3} \text{ Prim zu } 40$$

$$d \times 3 \% 40 = 1 \rightarrow \underline{\underline{d=27}}$$

Publickey: (3; 55)

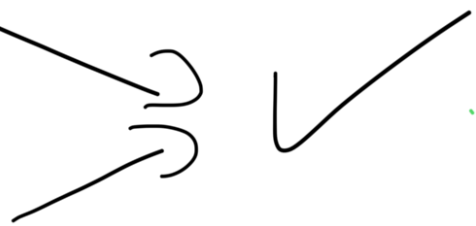
Privatekey: (27; 55)

Verschlüsselung:

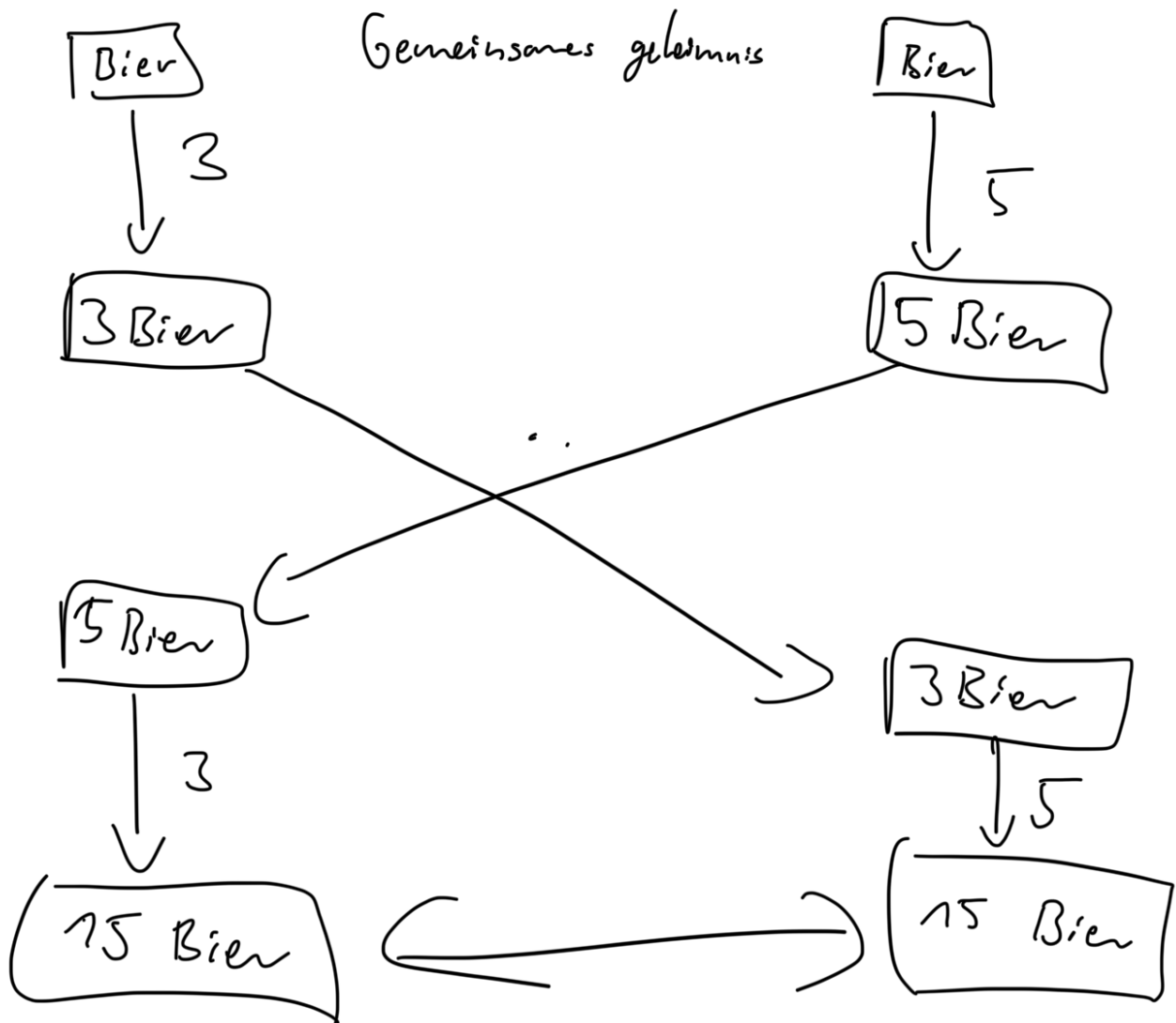
$$\underline{M=9} \rightarrow C = 9^3 \% 55 = 729 \% 55 = \underline{14}$$

Entschlüsseln:

$$M = 14^{27} \% 55 = \underline{9}$$



Diffie Hellmann



Zertifikate:

- Digitaler Ausweis

- Aussteller (CA)
- Eigentümer
- Gültigkeitszeitraum (von → bis)
- Public Key
- Signatur der CA

Browser: <https://laven.ddns.net> ✓

↓
Zertifikat ?

✓	X
---	---

↓
Aussteller (Lets Encrypt)

✓	X
---	---

inkäufliches
Vertrauen
notwendig

↓
→ Root CA

✓	X
---	---

Fire walls

→ Verwaltung und Steuerung von