RSA-Verfahren

Mathematische Grundlage

Joris Parthier 21.04.24

RSA-Verfahren

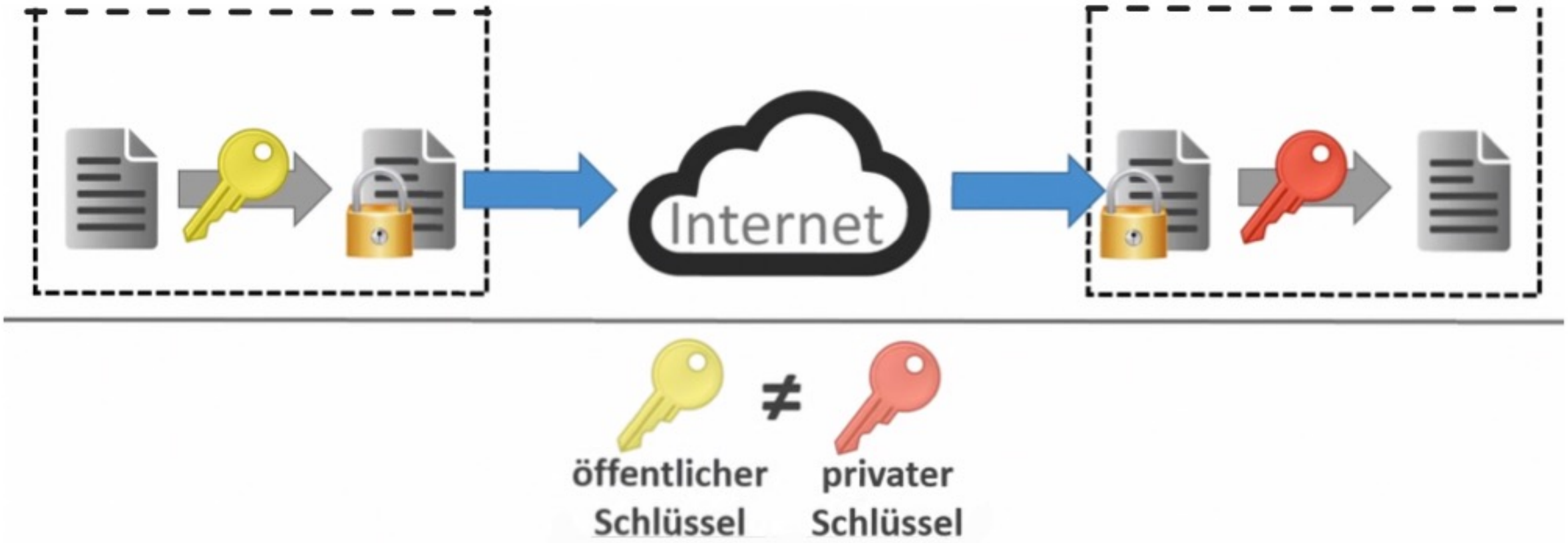
- **R**ivest, Ronald Linn
- **S**hamir, Adi
- **A**dleman, Leonard
- Entstehungsjahr :1977
- Asymmetrische Verfahren
- Einwegfunktion
- Kombination von Primzahlen

Besuche meine Website!

Für andere Erklärungsversuche und Resourcen

rsa-verfahren.github.io

Zur Darstellung



p = 7	q = 11	e = 13

Berechnung n: n = p * q = 7 * 11 = **77**

Berechnung m: m = (p-1) * (q-1) = (7-1) * (11-1) = **60**

Bestimmung e: e = 13
> Kriterium: Primzahl, aber kein Teil der Primzahlzerlegung von m, kleiner als m

Bestimmung d: d = 37
> Kriterium: Teilerfremd zu m, $0 < d$, $d * e \bmod m = 1$

Berechnung von d (Erweiterter Euklidischer Algorithmus)

e	m	e \ m	e mod m	a	b
13	**60**	0	13	**-23**	5
60	13	4	8	5	-23
13	8	1	5	-3	5
8	5	1	3	2	-3
5	3	1	2	-1	2
3	2	1	1	1	-1
2	1	2	0	**0**	**1**

$$B = a -(e\backslash m*b)$$

Berechnung von d

$d_{inkorrekt} = -23$ -> da aber gilt: $0 < d$

demnach:

$$d = d_{inkorrekt} + m = -23 + 60 = \underline{\underline{37}}$$

Formel Verschlüsselung:

$V = T^{e} \bmod n$

$V = T^{13} \bmod 77$

öffentlicher Schlüssel

n = 77, e = 13

Formel Entschlüsselung:

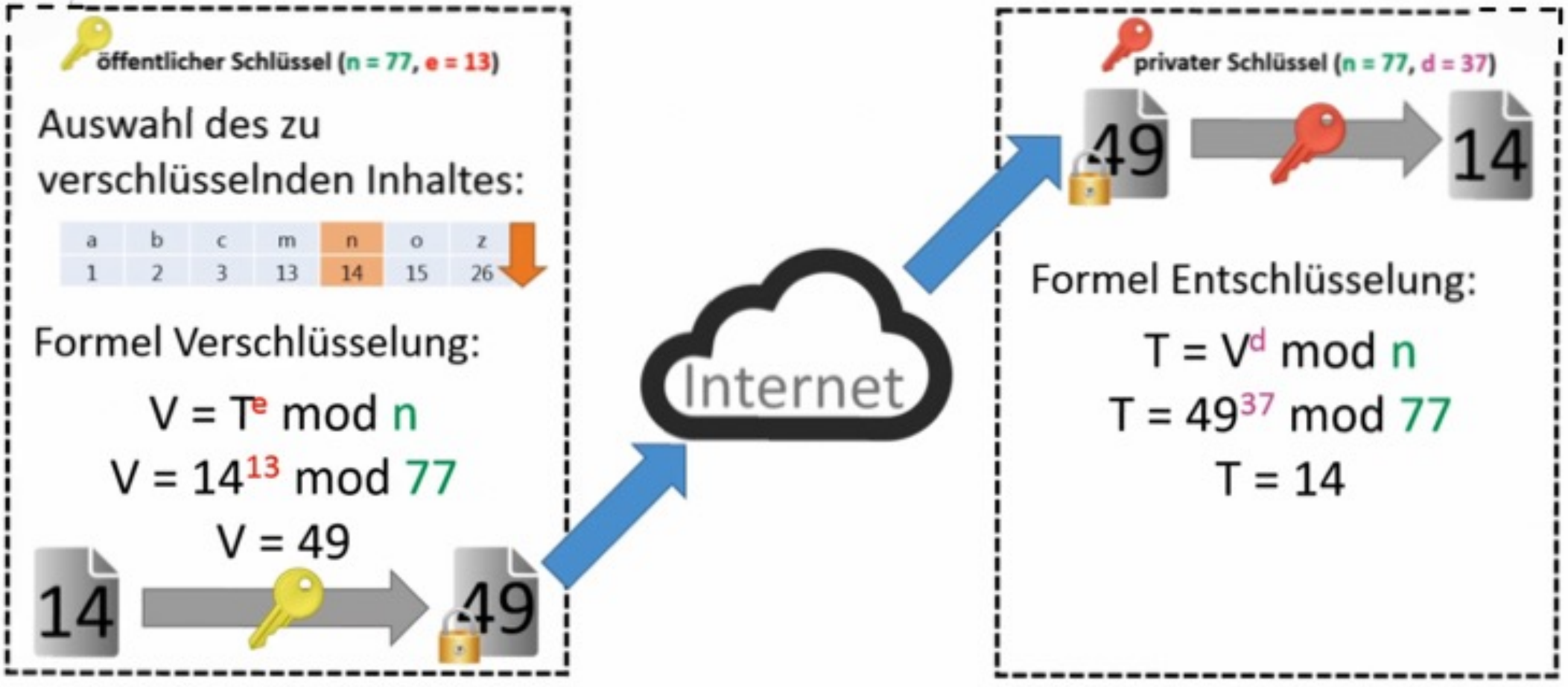
$T = V^{d} \bmod n$

$T = V^{37} \bmod 77$

privater Schlüssel

n = 77, d = 37

Zur Darstellung



Quellen:

rsa-verfahren.github.io

http://www.nord-com.net/h-g.mekelburg/krypto/mod-asym.htm#rsa

http://mitpress.mit.edu/sicp/psets/ps3/readme.html

https://youtu.be/XBanzOH02O4?si=mOjKiJBbtnrDXMyk

Besuche meine Website!

Für andere Erklärungsversuche und Resourcen

rsa-verfahren.github.io