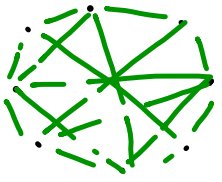
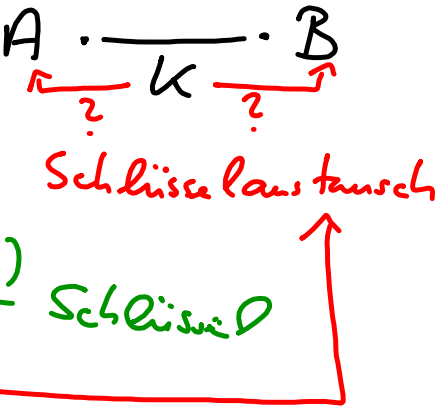
Public key Kryptographie

vorher: symmetrisch

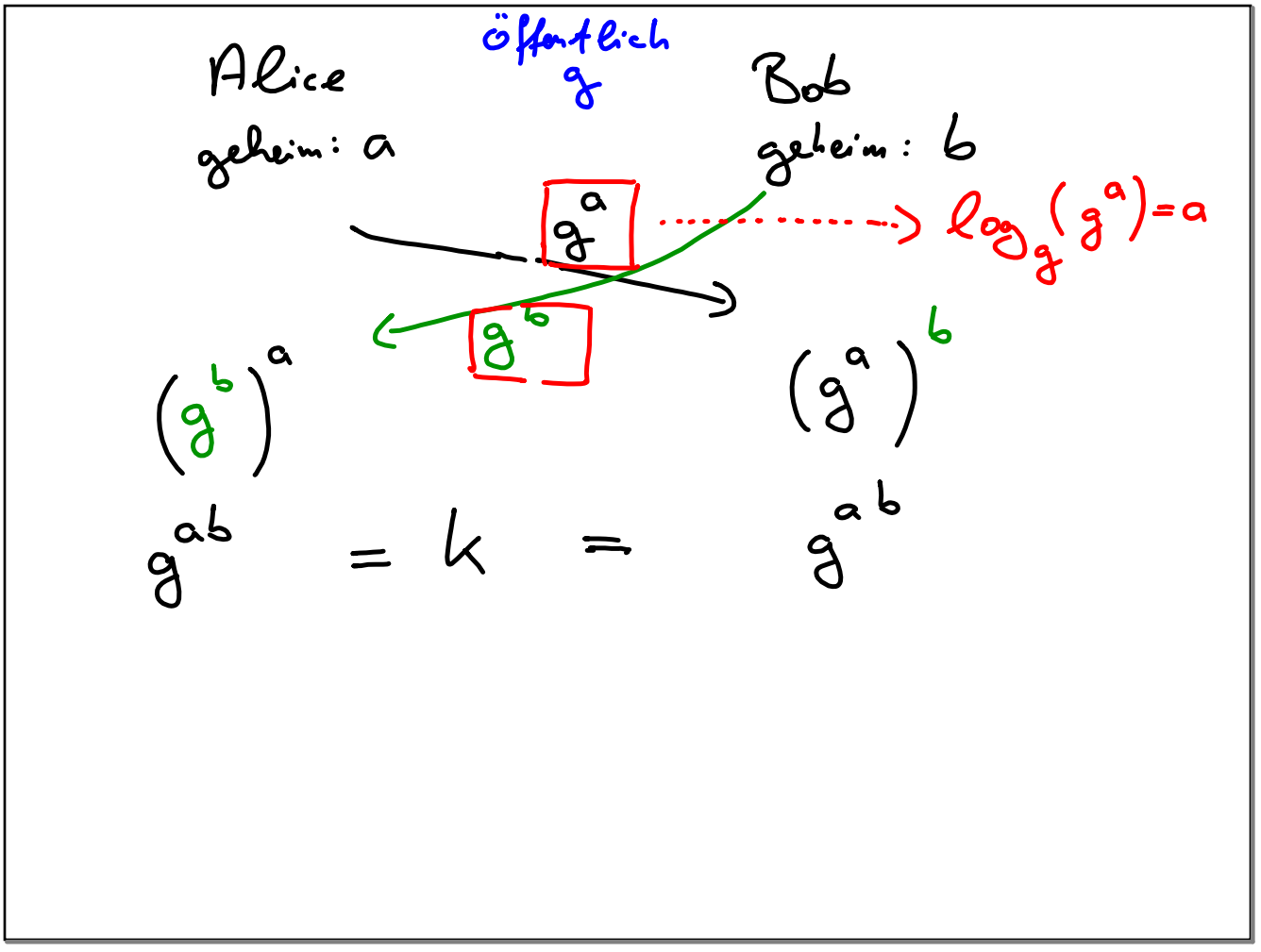


$\frac{n \cdot (n-1)}{2}$ Schlüssel



1976 Diffie-Hellman

1978 RSA erstes Public key System


Alice
geheim: a
öffentlich
g
Bob
geheim: b
g^a
$\log_g(g^a)=a$
g^b
$(g^b)^a$
$(g^a)^b$
$g^{ab} = k = g^{ab}$

Diffie und Hellman schlagen als Rechenbereich $\mathbb{Z}/p\mathbb{Z}$ vor, p Primzahl $p \in \mathbb{P}$

Modulare Arithmetik

$$22 + 8 \equiv 6 \pmod{24}$$

$$18 + 18 \equiv 12 \pmod{24}$$

$$2 \cdot 18 \equiv 12 \pmod{24}$$

$$6 - 8 \equiv 22 \pmod{24}$$

$$7 \cdot 11 \equiv 5 \pmod{24}$$

$$7 \equiv \frac{5}{11} \pmod{24}$$

"$D_0 + 5 = D_1$" $\rightarrow \mod 7$

$$3 + 5 \equiv 1 \pmod{7}$$

Mathematische Grundlage

Teilbarkeit:

$a \mid b$ für $a, b \in \mathbb{Z}$

$\Leftrightarrow \exists\, t \in \mathbb{Z}$ mit $a \cdot t = b$.

Modulo:

$a \equiv b \pmod{n}$ für $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$

$\Leftrightarrow n \mid (a-b)$

$6 \mid 18$

$2, 4 \in \mathbb{Z}$

$\frac{4}{2} \in \mathbb{Z}$

$3, 4 \in \mathbb{Z}$

$\frac{4}{3} \notin \mathbb{Z}$

Eigenschaften der mod-Relation

$n \in \mathbb{N}$ fest $\quad a \equiv b \pmod{n} \;\Big|\; a \sim b$

1) Reflexivität ✓ $a \sim a$

$a \equiv a \pmod{n}$

$\Leftrightarrow n \mid (a-a) \Leftrightarrow n \mid 0 \Leftrightarrow \exists t$ mit $n \cdot t = 0$ ($t = 0$) ✓

2) Symmetrie ✓ $a \sim b \Rightarrow b \sim a$

$a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b) \Leftrightarrow n \mid (b-a)$

$\Leftrightarrow b \equiv a \pmod{n}$

$n \mid a-b \Leftrightarrow n \cdot t = a-b \Leftrightarrow n \cdot t' = b-a \Leftrightarrow n \mid b-a$

$n \cdot t = -(b-a)$

$n \cdot (-t) = b-a$

3) Transitivität ✓ $a \sim b \wedge b \sim c \Rightarrow a \sim c$

$a \equiv b \pmod n \wedge b \equiv c \pmod n$

$n \mid a-b \wedge n \mid b-c$

$n \cdot t = a-b \wedge n \cdot t' = b-c$

$nt + nt' = a-c \Rightarrow n \cdot (t+t') = a-c$ ✓

$\Rightarrow \quad a \equiv b \pmod{n}$

ist eine Äquivalenzrelation

$\Rightarrow$ Klassenbildung möglich

die zu a äquivalenten Elemente liegen in der Klasse $[a]$

Beispiel: Klassen mod 3, d.h. $n = 3$

$n = 3$

$a = 1$

suche alle $b \in \mathbb{Z}$ mit

$b \equiv 1 \pmod 3$

$[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$

$[2] = \{\ldots -4, -1, 2, 5, 8 \ldots\}$

$[0] = \{\ldots -6, -3, 0, 3, 6 \ldots\}$

$[1] = [4]$

mod n gibt es n verschiedene Äq.-klassen

Menge $\mathbb{Z}/n\mathbb{Z}$ bezeichnet die Menge der Klassen

Mit den Klassen kann man +, −, · rechnen,

z.B. $[1]+[1]=[2]$

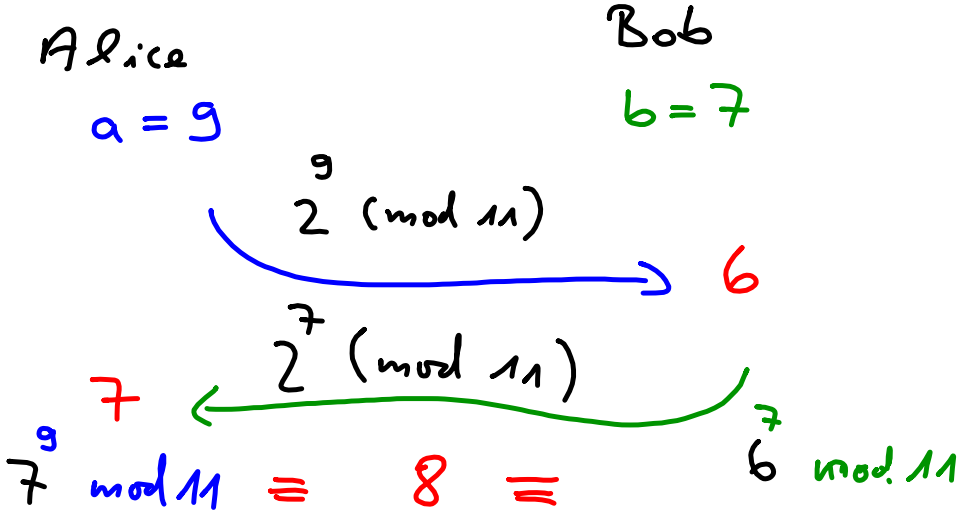
aber $[2]=[5]$, also auch $[1]+[1]=[5]$

Eindeutige Vertreter (mod n)

$[0], [1], [2], \ldots, [n-1]$

Beispiel zu Diffie-Hellman (mod p)

$p = 11$, $g = 2$



Übung:

mit PARI/GP

Diffie Hellman mit einer 16-Bit-Primzahl

$$2^7 \equiv \underbrace{2^4}_{16 \equiv 5 \bmod 11} \cdot \underbrace{2^3}_{8 \equiv -3 \bmod 11} \equiv 5 \cdot (-3) \equiv -15 \equiv 7 \bmod 11$$

$$2^9 \equiv 2^7 \cdot 2^2 \equiv 7 \cdot 4 \equiv 28 \equiv 6 \bmod 11$$