Digitale Signaturen

Georg Grasegger

Matheseminar, 9. Mai 2014

JOHANNES KEPLER
UNIVERSITÄT LINZ | JKU

talente
Stiftung

JKU Young Scientists
MATHEMATIK

Inhalt

Unterschrift

"Der Horizont vieler Menschen ist ein Kreis mit Radius Null - und das nennen sie ihren Standpunkt."

Euler/Einstein ?

Unterschrift

"Im rechtwinkligen Dreieck ist die Summe der Kathetenquadrate ungleich dem Hypotenusenquadrat."

Pythagoras ?

Probleme & Lösungen

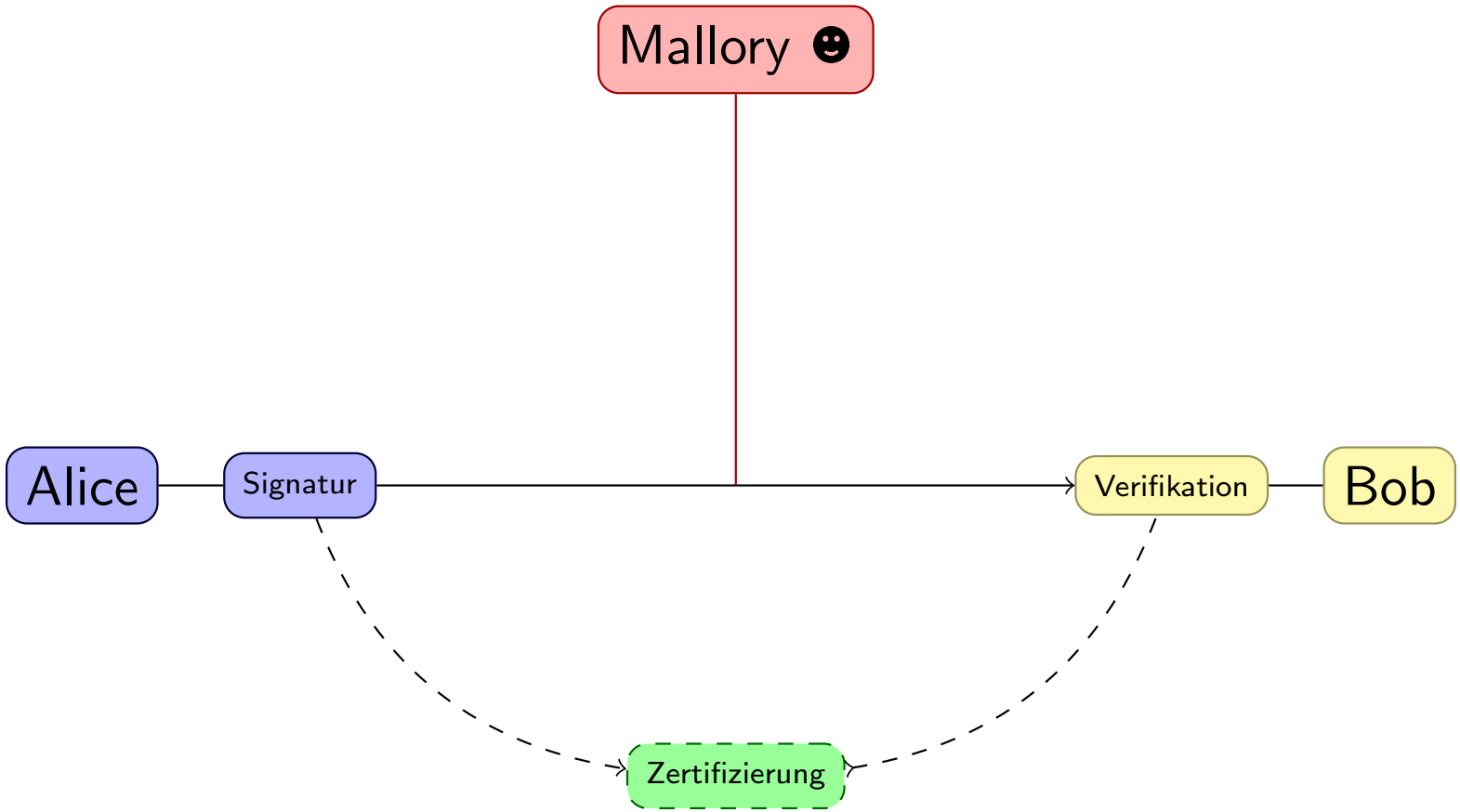
Probleme

- Falsche Nachricht
  - Phishing
  - Fälschungen
  - Identitätsdiebstahl
- Falsche Unterschrift
  - Mit fremden Federn schmücken
  - Copyright

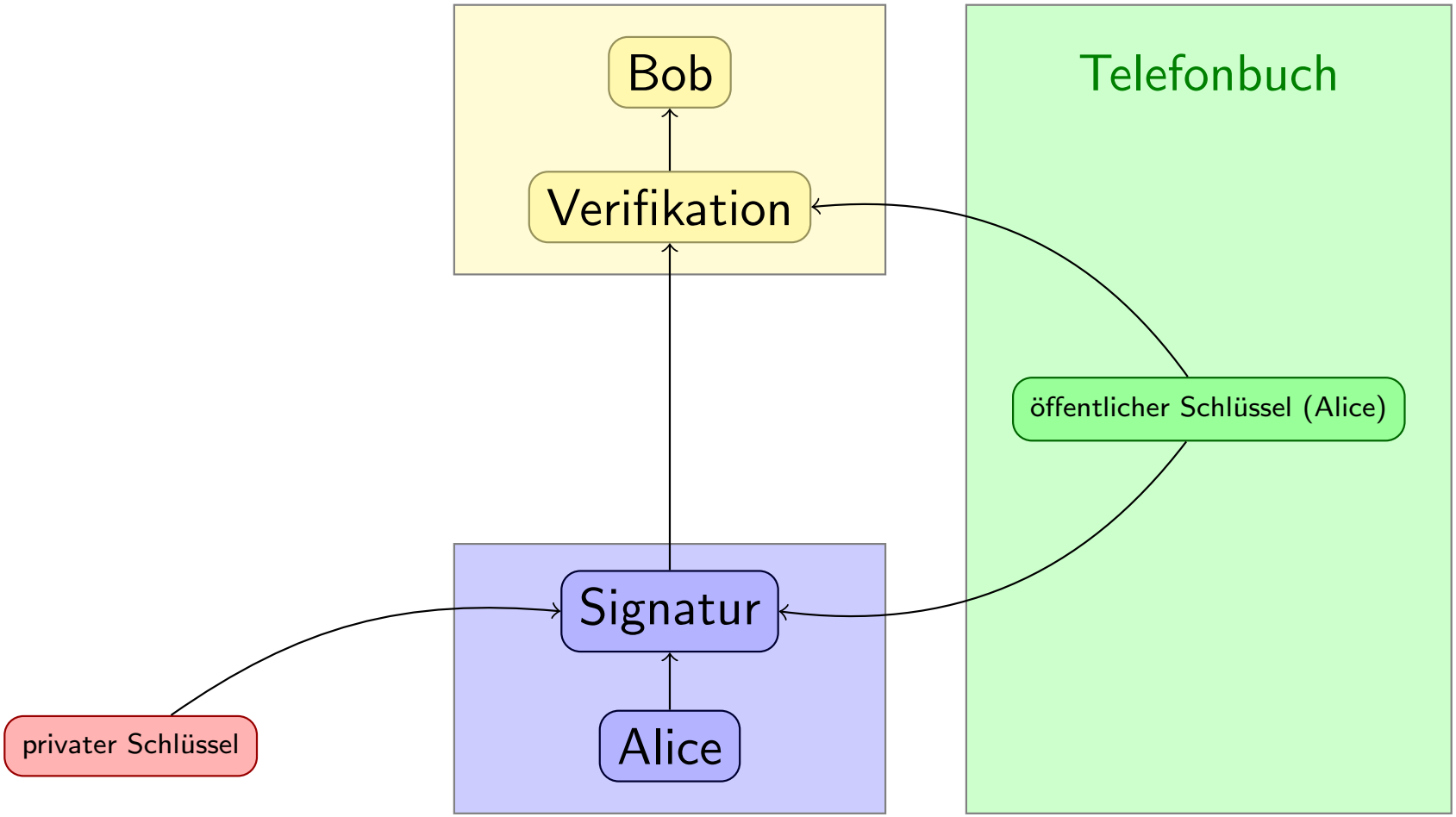
Lösung

- Digitale Signaturen
- Steganographie, Digitale Wasserzeichen

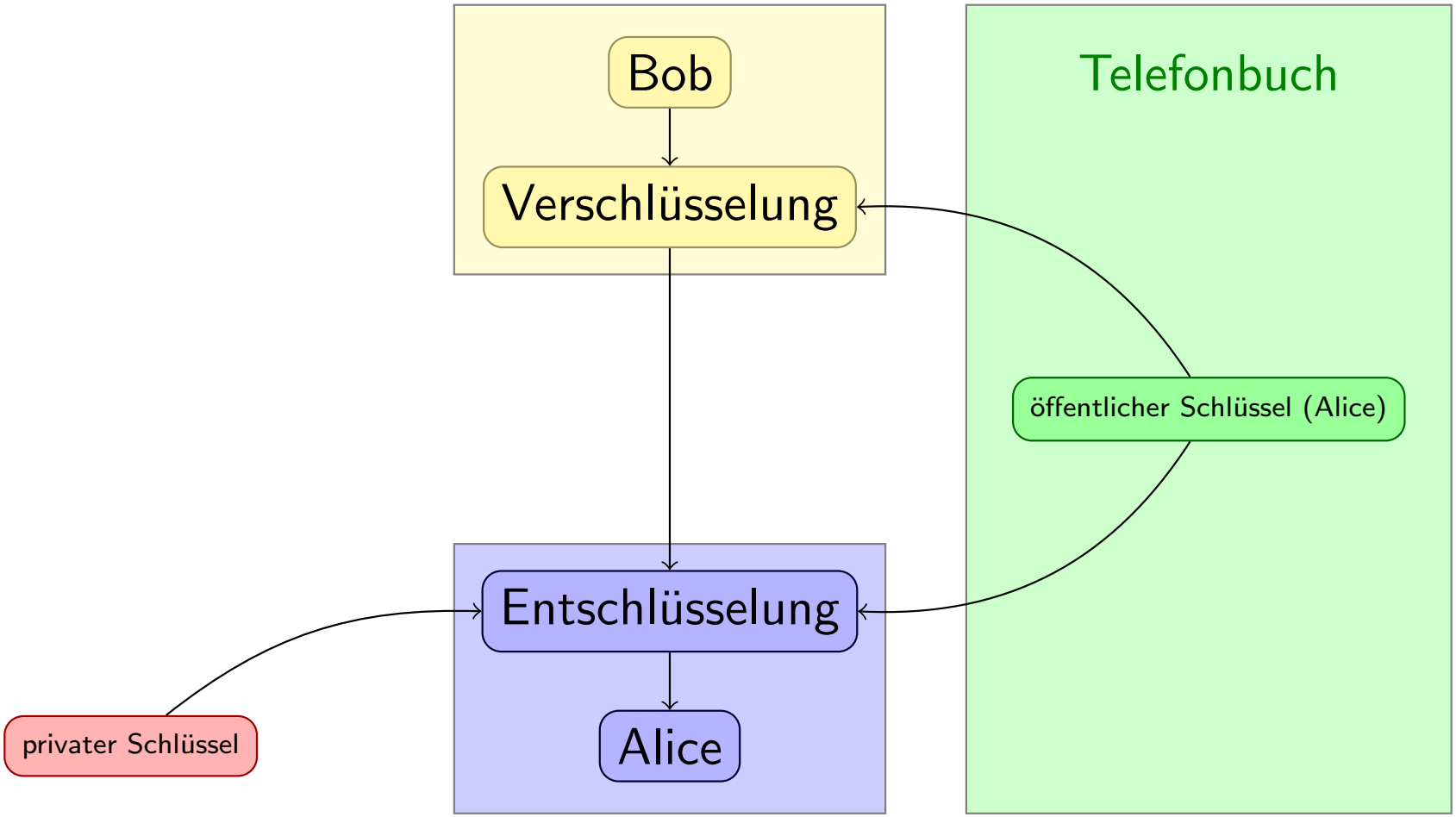
Ablauf



Funktionsweise

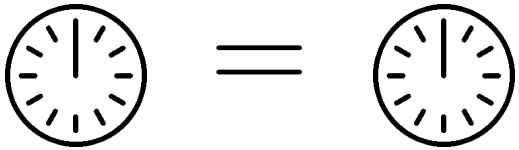


Funktionsweise

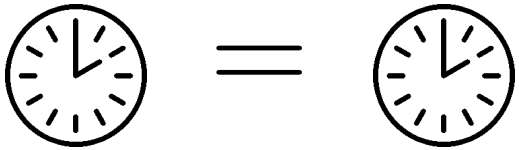


Inhalt

Modulo (I)

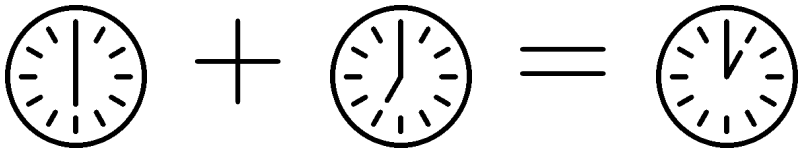


$$12 \equiv 0 \mod 12$$

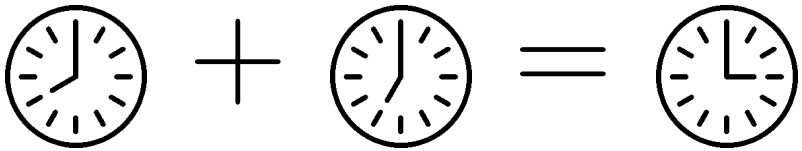


$$14 \equiv 2 \mod 12$$

Modulo (II)



$$6 + 7 \equiv 1 \mod 12$$



$$8 + 7 \equiv 3 \mod 12$$

Definition

Wir schreiben $a \equiv b \mod n$ genau dann, wenn $n \mid a - b$.

Wir haben dann folgende Rechenregeln

- Es gilt immer $a \equiv a \mod n$
- Wenn $a \equiv b \mod n$ dann gilt auch $b \equiv a \mod n$
- Wenn $a \equiv b \mod n$ und $b \equiv c \mod n$, dann gil auch $a \equiv c \mod n$

Weiters

- Für jedes a gibt es genau ein $0 \leq b < n$, sodass $a \equiv b \mod n$

Aufgaben

Addition

$$7 + 2 \equiv ? \mod 11 \qquad 25 + 31 \equiv ? \mod 7 \qquad 102 + 123 \equiv ? \mod 3$$
$$7 + 12 \equiv ? \mod 7 \qquad 45 + 14 \equiv ? \mod 11 \qquad 156 + 122 \equiv ? \mod 5$$

Subtraktion

$$10 - 5 \equiv ? \mod 2 \qquad 3 - 15 \equiv ? \mod 3 \qquad 5 - 7 \equiv ? \mod 9$$
$$-10 \equiv ? \mod 3 \qquad 5 - 15 \equiv ? \mod 5 \qquad 5 - 13 \equiv ? \mod 3$$

Multiplikation

$$5 \cdot 3 \equiv ? \mod 7 \qquad 15 \cdot 13 \equiv ? \mod 10 \qquad 12 \cdot (-3) \equiv ? \mod 5$$
$$2 \cdot 2 \equiv ? \mod 4 \qquad 12 \cdot 12 \equiv ? \mod 13 \qquad 153 \cdot 237 \equiv ? \mod 4$$

PowerMod

Potenzieren

Wir wollen $5^{21} \mod 7$ berechnen.

$$\begin{aligned} 5^{21} &\equiv 5 \cdot 5^{20} \equiv 5 \cdot (5^2)^{10} \equiv 5 \cdot 25^{10} \equiv 5 \cdot 4^{10} \equiv 5 \cdot (4^2)^5 \\ &\equiv 5 \cdot 16^5 \equiv 5 \cdot 2^5 \equiv 5 \cdot 2 \cdot 2^4 \equiv 10 \cdot (2^2)^2 \equiv 3 \cdot 4^2 \\ &\equiv 3 \cdot 16 \equiv 3 \cdot 2 \equiv 6 \mod 7 \end{aligned}$$

Kleiner Satz von Fermat

Satz (Fermat)

Sei $p \in \mathbb{P}$. Dann gilt für alle $a \in \mathbb{Z}$

$$a^p \equiv a \mod p\,.$$

Falls $p \nmid a$, gilt auch

$$a^{p-1} \equiv 1 \mod p\,.$$

Beispiel (Forts.)

$$5^{21} \equiv 5^{18+3} \equiv 5^{18} \cdot 5^3 \equiv (5^6)^3 \cdot 5^3 \equiv 1^3 \cdot 5 \cdot 25 \equiv 5 \cdot 4 \equiv 6 \mod 7$$

Kleiner Satz von Fermat

Aufgabe

$$5^{101} \mod 11 \qquad 7^{221} \mod 13 \qquad 16^{4} \mod 17$$
$$(-2)^{29} \mod 5 \qquad 312^{130} \mod 3 \qquad 3^{13} \mod 4$$

Erweiterter euklidischer Algorithmus

$$\text{ggT}(x, y) = ax + by$$

		a	b	
I	96	1	0	
II	13	0	1	
III	5	1	-7	I-7II
IV	3	-2	15	II-2III
V	2	3	-22	III-IV
VI	1	-5	37	IV-V
VII	0	–	–	V-2VI

Aufgabe

$\text{ggT}(101, 11)$

$\text{ggT}(25, 14)$

$\text{ggT}(15, 56)$

$\text{ggT}(6, 33)$

$\text{ggT}(30, 7)$

$\text{ggT}(20, 5)$

Inverse

Gegeben: $p \in \mathbb{P}$ und $x \in \mathbb{Z}_p$

Gesucht: $y \in \mathbb{Z}_p$, sodass $xy \equiv 1 \mod p$
(wir schreiben $y = x^{-1}$)

Methode:

- Berechne $\text{ggT}(x, p) = ax + bp$.
- Da $p \in \mathbb{P}$, folgt $\text{ggT}(a, p) = 1$.
- Also $1 = ax + by \equiv ax \mod p$

Aufgabe

$3^{-1} \mod 5$ $\quad$ $5^{-1} \mod 17$ $\quad$ $7^{-1} \mod 31$

Modulo in Computer-Algebra-Systemen

	$a \mod p$	$a^x \mod p$	$\mathrm{ggT}(a,b)$
Mathematica	`Mod[a,p]`	`PowerMod[a,x,p]`	`GCD[a,b]`
WolframAlpha	`a mod p`	`a^(x) mod p`	`gcd a b`
Maxima	`mod(a,p)`	`power_mod(a,x,p)`	`gcd(a,b)`
Sage	`mod(a,p)`	`a.powermod(x,p)`	`gcd(a,b)`
GeoGebra	`Mod[a,p]`	`Mod[a^x,p]`	`GGT[a,b]`

Inhalt

Schlüssel

- $p \in \mathbb{P}$
- $g \in \mathbb{Z}_p^*$
- $x \in \mathbb{Z}_p^*$
- $y \equiv g^x \mod p$
- Öffentlicher Schlüssel: (p, g, y)
- Privater Schlüssel: x

- $p = 17$
- $g = 3$
- $x = 5$
- $y \equiv 3^5 \equiv 5 \mod 17$
- $(17, 3, 5)$
- 5

Aufgabe

Erstelle einen privaten und einen öffentlichen Schlüssel.

Achtung! Der private Schlüssel muss unbedingt geheim bleiben.

Signatur

- Zur Verfügung: alle Schlüssel
- Nachricht: $m \in \mathbb{Z}_p$
- Wähle $1 < k < p-1$, sodass $\text{ggT}(k, p-1) = 1$
- $r \equiv g^k \mod p$
- $s \equiv (m - xr)k^{-1} \mod p-1$
- Signatur: (r, s)

- $(p, g, y) = (17, 3, 5)$, $x = 5$
- $m = 6$
- $k = 11$ $\text{ggT}(11, 16) = 1$
- $r = 7$
- $s = 9$
- $(7, 9)$

Aufgabe

Signiere eine Nachricht und "versende" sie.

Verifikation

- Zur Verfügung: öffentlicher Schlüssel (p, g, y)
- Erhalten: m und (r, s)
- Überprüfe:
  - $0 < r < p$
  - $0 < s < p - 1$
  - $g^m \equiv y^r r^s \mod p$

- $(17, 3, 5)$
- 6 und $(7, 9)$
-
  - $0 < 7 < 17$
  - $0 < 9 < 16$
  - $g^m \equiv y^r r^s \equiv 15 \mod 17$

Aufgabe

Verifiziere die erhaltene Nachricht.

Aufgabe

Korrektheit

Zeige, dass bei einer korrekten Signatur, die Gleichung $g^m \equiv y^r r^s \mod p$ erfüllt ist.

Sicherheitsrisiken

Aufgabe

Alice hat eine signierte Nachricht verschickt. Aus versehen hat sie aber auch noch die Zahl k veröffentlicht. Wie kann Mallory diese Tatsache nutzen um an den privaten Schlüssel von Alice zu gelangen?

Aufgabe

Alice hat zwei verschiedene Nachrichten signierte und dabei aber jeweils das gleiche k verwendet. Wie kann Mallory mit diesem Wissen an den privaten Schlüssel von Alice gelangen?

Öffentliches k

- Gegeben: (p, g, y), m, (r, s) und k
- Gesucht: x
- Annahme: $\mathrm{ggT}(r, p-1) = 1$

$$x \equiv (m - sk)r^{-1} \mod p - 1$$

Gleiches k

- Gegeben: (p, g, y), m_1, (r, s_1) und m_2, (r, s_2)
- Gesucht: k
- Annahme: $\mathrm{ggT}(s_1 - s_2, p - 1) = 1$

$$k \equiv (m_1 - m_2)(s_1 - s_2)^{-1} \mod p - 1$$

da

$$g^{m_1} \equiv y^r r^{s_1} \equiv y^r g^{k s_1} \mod p$$
$$g^{m_2} \equiv y^r r^{s_2} \equiv y^r g^{k s_2} \mod p$$

Angriffe (I)

- Gegeben: (p, g, y)
- Gesucht: x
- Wir wissen: $y \equiv g^x \mod p$
- Diskreter Logarithmus

Hacker-Wettbewerb

Finde ohne Hilfe eines Computers die privaten Schlüssel, die zu den öffentlichen Schlüsseln $(31, 3, 30)$, $(31, 2, 1)$, $(71, 10, 3)$, $(541, 5, 125)$ passen und mit Hilfe eines Computers die privaten Schlüssel von $(107, 92, 40)$ und $(113, 101, 42)$. Was fällt auf?