Repe Krypto

- Hash
- DH
- Symmetische Krypto
- Asymmetische Krypto
  - Verschlüsselung
- Digitale Unterschrift
- Authentifikation

Hash

beliebige Bitfolge

bekannte "Formel"

konstante Bitlänge

unmöglich

1 Bit ändern

"zufällig" etwa die Hälfte der Bits ändert

Anwendung Hashes

- Digitale Clientsdrift (Baustein)

- Plagiatsprüfung
- Abspeichern von Passworthashes

- Datenintegrität (technische Fehler)

Diffie-Hellmann Key Exchange

$a \star b = r$

Aus r, a kann b nicht bestimmt werden.

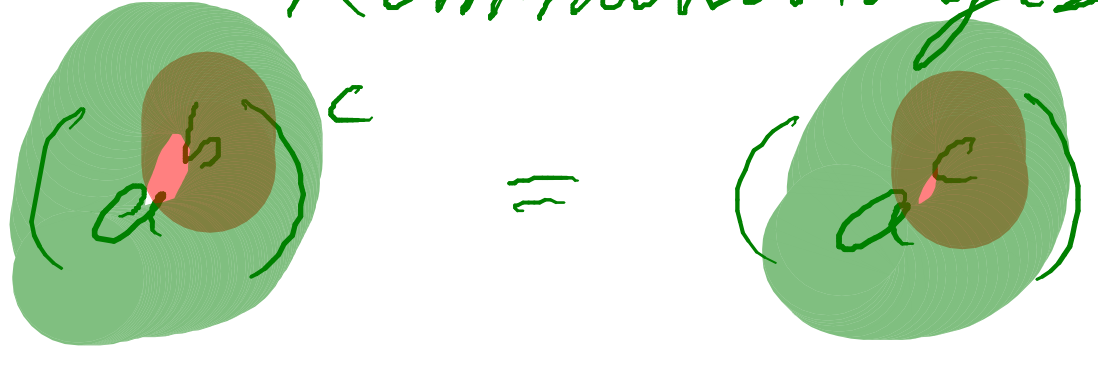
$(a \star b) \star c = a \star (b \star c)$

Assoziativgesetz.

$(a \star b) \star c = (a \star c) \star b$

Kommutativgesetz

z.B. $(a^b)^c = (a^c)^b$



Alice

Bob

p : primzahl

a : geheim

b : Basis

p

c : geheim

b

$b \bmod p$

$b^c \bmod p$

$(b^c)^a \bmod p$

$b^{a \cdot c}$

Passwort

$(b^a)^c \bmod p$

$b^{a \cdot c}$

Symetische Krypto

gemeinsames Password
(Schlüssel)

kann ver- und
entschlüsseln.

AES

128 Bit Schlüssel
256 Bit Variante

Asymmetrische Krypto

Public/private key

öffentlicher Schlüssel o

privater Schlüssel p

$$(x \boxtimes o) \boxtimes p = x$$

$$(x \boxtimes p) \boxtimes o = x$$

RSA (mod n)

$$(x^o)^p = x$$

$$(x^p)^o = x$$

$x < n$

Verschlüsselung

n : 4096 Bits

passwort × 128 / 256 Bit

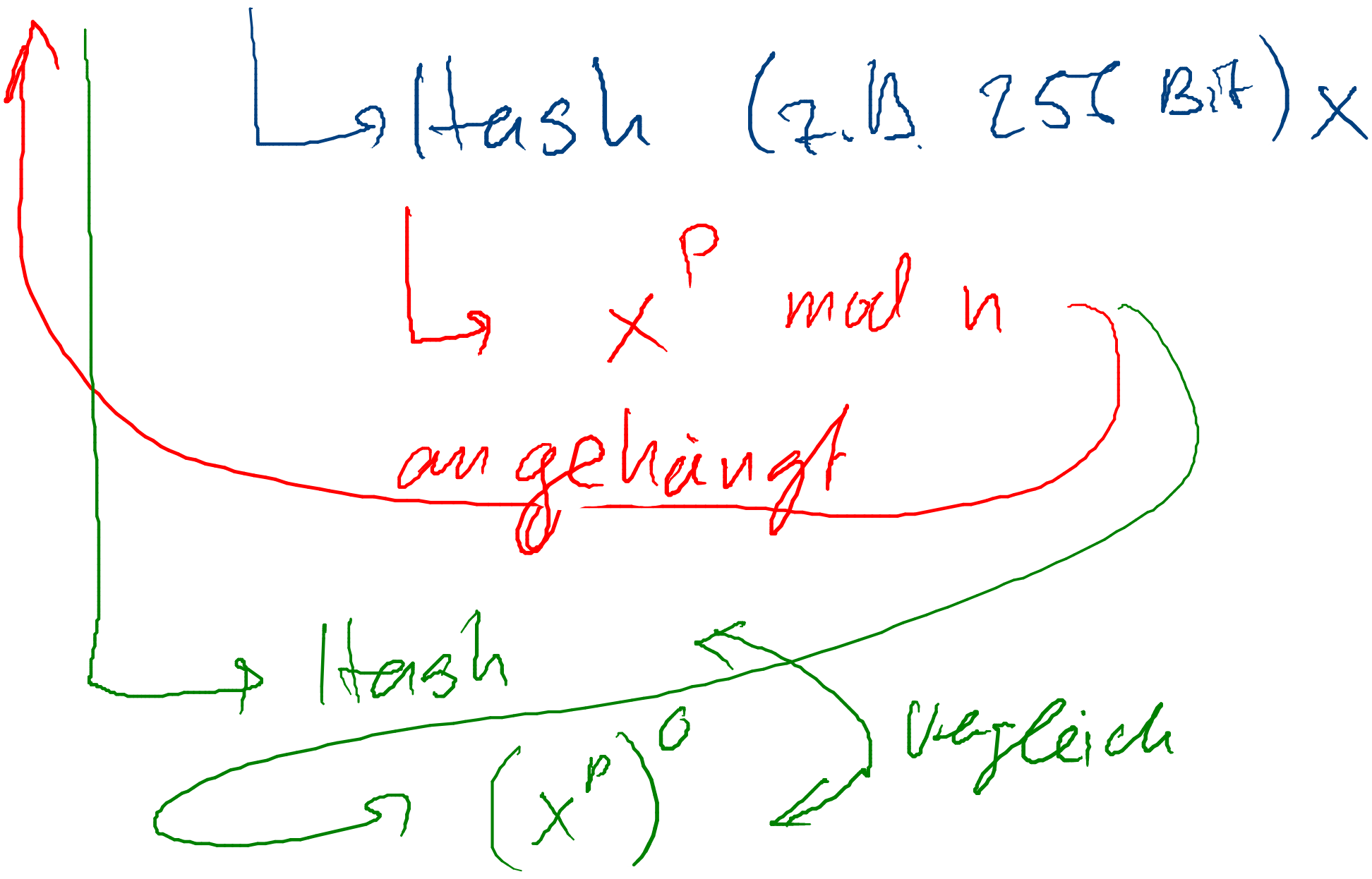
↳ Verschlüsselt.

mit x^0 mod n

↳ x wird zum Verschlüsseln (symetrisch) von der Nachricht gebraucht

Digitale Unterschrift

Dokument



Authentifikation

CA : Certificate Authorities

unterschreiben anderen

öffentliche Schlüssel.

Web of trust

Modulus $n = p \cdot q_1$

↑ ↑

prim prim

$p \cdot q_2$

A^{16}

$72?$

Hausaufgabe:

Schlüssel generieren

mit e-mail senden

mit öffentlichem Schlüssel.