Verschlüsselung und Signatur mit DL

ElGamal ~ 1980

Verschlüsselung einer Nachricht m

p Primzahl, Rechnen mod p, $0 \le m \le p-1$

pro Teilnehmer

geheim:

a mit $2 \le a \le p-2$

öffentlich:

$p \in \mathbb{P}$, Erzeuger g, $y \equiv g^a \bmod p$

Senden von m an Teilnehmer:

- Zufallszahl k
- $\left(\underbrace{g^k \bmod p}_{c}, \underbrace{m \cdot y^k \bmod p}_{d} \right)$
- Chiffretext (c, d)

Entschlüsseln eines Chiffretextes

$$m \equiv c^{p-1-a} \cdot d \bmod p$$

$$\left(g^k\right)^{p-1-a} \cdot m \cdot y^k \equiv \left(g^{p-1}\right)^k \cdot g^{-ak} \cdot m \cdot \left(g^a\right)^k$$

$$\equiv m \bmod p$$

($g^{p-1} \equiv 1$, $g^{-ak} \cdot \left(g^a\right)^k \equiv 1$)

Übung:

$p = 23$, $g = 5$, $a = 7$, $y = ?$

ist Schlüssel eines Teilnehmers

p, g, y öffentlich

a geheim

Verschlüsseln von $m = 6$ mit $k = 9$ (Zufallszahl).

+ Entschlüsselung

Bemerkung:

- p sichere Primzahl mit Länge ≥ 2048 Bit

- Verschlüsselung langer Nachrichten
  - blockweise, nicht praktikabel
  - verschlüssele symmetrischen Schlüssel k und verschlüssele m mit einem symmetrischen Verfahren mit k