Pollard-ρ für 30-bit

$p = 941531387$

$g = 2$

$p - 1 = 2 \cdot q$

$2^x \equiv 3 \mod p$

BigInteger

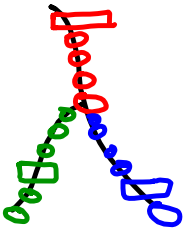
2 — q

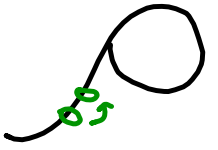
$(2^x)^{\frac{p-1}{q}} \equiv 3^{\frac{p-1}{q}} \mod p$

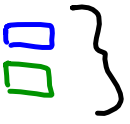
$4^x \equiv 9 \mod p$

Parallelisierung der Pollard-Methode

$y = g^k \cdot h^l = g^{k'} \cdot h^{l'}$

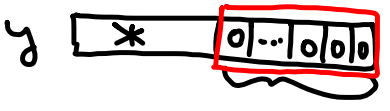






gesendeten Zwischenergebnisse

(Server sammelt y, k, l)



$1 : 2^{20}$

DISTINGUISHED POINT

Client i hat eigenen Startwert

$y \equiv g^{k_i} h^{l_i} \bmod p$ zufällig gewählt

Verschlüsselung von ElGamal

Public key Verfahren

Public key eines Teilnehmers

p sichere Primzahl ($p-1$ hat großen Primteiler $q > 2^{1024}$)

g Erzeuger mod p

y $(\equiv g^a \bmod p)$

z.B. $p-1 = 2 \cdot q$

Secret key

Zufallszahl a mit $2 \leq a \leq q-2$

Nachricht an den Teilnehmer senden

$0 \leq m \leq p-1$

1.) (p, g, y) des Teilnehmers lesen

2.) Zufallszahl k mit $2 \leq k \leq q-2$

3.) $c = g^k \bmod p$, $d \equiv m \cdot y^k \bmod p$

(c, d) ist verschlüsselte Nachricht

Entschlüsselung

1.) erhalte verschlüsselte Nachricht (c, d)

2.) berechne

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

Warum erhält man wieder den Klartext?

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

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

$$g^{p-1} \equiv 1 \mod p$$

$$\equiv \underbrace{\left(g^{p-1}\right)^k}_{1} \cdot \underbrace{g^{-ak}}_{} \cdot m \cdot \underbrace{g^{ak}}_{} \mod p \equiv m \mod p$$

✓

Übung: ElGamal-Implementierung mit 2048-bit Primzahl p

RSA

Public key System von Rivest, Shamir, Adleman

1978

Public key

$n = p \cdot q$

e zufällig $\quad 2 \leq e \leq \varphi(n) - 2$

$\varphi(n) = (p-1) \cdot (q-1)$

Secret key

p, q } Primzahlen $> 2^{1024}$

$d \equiv \frac{1}{e} \bmod (p-1) \cdot (q-1)$

Verschlüsseln einer Nachricht m

$m' \equiv m^e \bmod n$

Entschlüsseln einer Nachricht m'

$m \equiv m'^d \bmod n$