zu Übungsaufgabe

Schlüssel

mit 10^4 CPUs, 3,6 GHz,

in 1 Jahr

$1,1 \cdot 10^{21}$

Erzeuger finden

Ordnung eines Elements mod p ist ein Teiler von $p-1$

$\Rightarrow$ effizientes Erzeuger-Kriterium

Zerlegung von $p-1$ in Primfaktoren

$$p-1 = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}$$

g ist ein Erzeuger, wenn

$$g^{\frac{p-1}{q_i}} \not\equiv 1 \mod p \qquad 1 \le i \le r$$

Übung:

1) 3 ist Erzeuger mod 7

$p-1 = 6 = 2 \cdot 3 \Rightarrow q_1 = 2, q_2 = 3$

q_1 ↓ a), q_2 ↓ b)

Prüfe

a) $3^{\frac{7-1}{2}} \equiv 3^3 \equiv 9 \cdot 3 \equiv 2 \cdot 3 \equiv 6 \bmod 7$

$6 \not\equiv 1$

b) $3^{\frac{7-1}{3}} \equiv 3^2 \equiv 9 \equiv 2 \bmod 7$

$2 \not\equiv 1$

$\Rightarrow$ 3 ist Erzeuger

2) $p = 13$, finde Erzeuger

teste $g = 2$:

$p-1 = 13-1 = 12 = 2^2 \cdot 3$

$\Rightarrow q_1 = 2, q_2 = 3$

$2^{\frac{13-1}{2}} \equiv 2^6 \equiv 2^4 \cdot 2^2 \equiv 3 \cdot 4 \equiv 12 \bmod 13$ ✓

$2^{\frac{13-1}{3}} \equiv 2^4 \equiv 3 \bmod 13$ ✓

$\Rightarrow$ 2 ist Erzeuger

3) $p = 17$, finde Erzeuger

teste $g = 2$

$p - 1 = 17 - 1 = 2^4 \Rightarrow q_1 = 2$

$2^{\frac{17-1}{2}} \equiv 2^8 \equiv 2^4 \cdot 2^4 \equiv \underbrace{16 \cdot 16} \equiv 1 \mod 17$

$(-1) \cdot (-1) \equiv 1$

$\Rightarrow$ 2 kein Erzeuger mod 17

teste $g = 3$

$3^{\frac{17-1}{2}} \equiv 3^8 \equiv \underbrace{3^3}_{10} \cdot \underbrace{3^3}_{10} \cdot 3^2 \equiv 100 \cdot 9$

$\equiv (-2) \cdot 9 \equiv -18 \equiv 16 \mod 17$

$\not\equiv 1$ ✓

$\Rightarrow$ 3 ist ein Erzeuger

4) $p = 19$, Erzeuger suchen

$19 - 1 = 18 = 2 \cdot 3^2 \quad q_1 = 2, q_2 = 3$

$2^{\frac{19-1}{2}} \equiv 2^8 \equiv 2^4 \cdot 2^4 \cdot 2 \equiv (-3) \cdot (-3) \cdot 2$

$\equiv 18 \mod 19$ ✓

$2^{\frac{19-1}{3}} \equiv 2^6 \equiv 2^4 \cdot 2^2 \equiv (-3) \cdot 4$

$\equiv -12 \equiv 7 \mod 19$ ✓

$\Rightarrow$ 2 Erzeuger mod 19

Sichere Primzahlen finden

Voraussetzung:

ein q_i in der Zerlegung von $p-1$ muss "groß" sein.

"groß" = mind. 10^{50} bzw. 160 Bits

Spezialfall: p Primzahl

$$q = \frac{p-1}{2} \text{ Primzahl}$$

(Primzahl q heißt Sophie-Germain-Primzahl)

Beispiele für solche p:
5, 11, 23, 47, ...

Übung:

Implementierung Diffie-Hellman

Attacken auf Diffie-Hellman Schlüsselaustausch

Methode von Shanks:

Löse Gleichungen der Form

$$g^x \equiv h \mod p$$

mit folgendem Trick

$$x = x_0 + x_1 \cdot m$$

$$m = \lceil \sqrt{p} \rceil$$

und $0 \leq x_0 \leq m$, $0 \leq x_1 \leq m$

Idee:

(I) Tabelle mit Hilfe von $0 \leq x_0 \leq m$

(II) Lookup in Tabelle für $0 \leq x_1 \leq m$

$$g^{x_0 + x_1 \cdot m} \equiv h \mod p$$

$$g^{x_0} \cdot g^{x_1 m} \equiv h \mod p$$

$$\underbrace{\left(g^m\right)^{x_1}}_{(II)} \equiv \underbrace{h \cdot g^{-x_0}}_{(I)} \mod p$$

Beispiel:

$p = 13, \quad g = 2, \quad h = 6$

$$2^x \equiv 6 \mod 13$$

$m = \lceil \sqrt{13} \rceil = 4$

$x = x_0 + x_1 \cdot 4 \quad$ mit $\quad 0 \leq x_0 \leq 4$

$0 \leq x_1 \leq 3$

zu (I):

Hashtabelle für x_0

x_0	$h \cdot g^{-x_0} \mod 13$
0	6
1	3
2	8
3	4
4	2

$h \cdot g^{-x_0}$

$6 \cdot 2^{-0} \equiv 6$

$6 \cdot 2^{-1} \equiv 3$

$6 \cdot 2^{-2} \equiv$

$6 \cdot 7^2$

zu (II):

$(g^m)^{x_1}$ für $x_1 = 0, 1, 2, \ldots$ in Tab. suchen

$g^m \equiv 2^4 \equiv 3 \mod 13$

$(g^m)^0 \equiv 1 \mod 13 \notin$ Tab.

$(g^m)^1 \equiv 3^1 \equiv 3 \mod 13 \in$ Tab

$\Rightarrow x_1 = 1$ ist Treffer mit $x_0 = 1$

$\Rightarrow x = x_0 + x_1 \cdot m = 1 + 1 \cdot 4 = 5$