Angriffe auf DL-Systeme

DL: diskreter Logarithmus

Ausprobieren (brute force):

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

$O(\log^2 p)$

$g^0, g^1, g^2, \ldots \mod p$ max $p-1$ Mult. mod p

$O(p \cdot \log^2 p)$ polynomiell?

Eingabelänge der Zahl p ist $\log_2(p)$.

$$p = 2^{\log_2(p)}$$

$$\Theta(p \cdot \log^2 p) = \Theta(2^{\log_2(p)} \cdot \log^2 p)$$

exponentielle Laufzeit $\Theta(\ell^2 \cdot 2^{\ell})$

Idee von Pohlig und Hellman

Zerlege das Originalproblem auf

Teiler von $p-1 = q_1^{e_1} \cdot q_2^{e_2} \cdots q_k^{e_k}$, $q_i \in \mathbb{P}$

$$\left(g^{x_i}\right)^{\frac{p-1}{q_i}} \equiv h^{\frac{p-1}{q_i}} \mod p$$

$\rightsquigarrow$ $x_i \in \{0, 1, \ldots, q_i - 1\}$, $1 \leq i \leq k$

es gilt

$$x \equiv x_i \mod q_i$$

$$g^{\frac{p-1}{q_i}} \not\equiv 1 \mod p$$

Beispiel:

$$p = 31\,,\quad p-1 = 2\cdot 3\cdot 5\,,\quad g = 3$$

$$3^x \equiv 22 \mod 31$$

$q_1 = 2$:

$$\left(3^x\right)^{\frac{31-1}{2}} \equiv 22^{\frac{31-1}{2}} \mod 31$$

$$30^x \equiv 30 \mod 31 \Rightarrow x \equiv 1 \mod 2$$

$q_2 = 3$:

$$\left(3^x\right)^{\frac{31-1}{3}} \equiv 22^{\frac{31-1}{3}} \mod 31$$

$$\boxed{25^2 \equiv (-6)^2 \equiv 36 \equiv 5 \mod 31}$$

$$25^x \equiv 5 \mod 31 \Rightarrow x \equiv 2 \mod 3 \checkmark$$

$q_2 = 5$:

$$3^x \equiv 22 \mod 31$$

$$\left(3^x\right)^{\frac{31-1}{5}} \equiv 22^{\frac{31-1}{5}} \mod 31$$

$$16^x \equiv 8 \mod 31$$

$$16^2 \equiv \left(2^4\right)^2 \equiv 2^8 \equiv \underbrace{2^5}_{1} \cdot 2^3 \equiv 8 \mod 31$$

$\Rightarrow x \equiv 2 \mod 5$

$$\underbrace{\left.\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv 2 \mod 3 \\ x &\equiv 2 \mod 5 \end{aligned}\right\} \quad x \equiv 17 \mod p-1}_{\text{chinesischer Restsatz (CRT)}}$$

Systematische Bestimmung der CRT-Lösung

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \end{aligned} \qquad x = a_1 \cdot m_2 \cdot m_2' + a_2 \cdot m_1 \cdot m_1'$$

Ziel: $m_1 \cdot m_1' \equiv 1 \mod m_2$

$$\Rightarrow \quad m_1' \equiv \frac{1}{m_1} \mod m_2$$

$$m_2 \cdot m_2' \equiv 1 \mod m_1$$

$$m_2' \equiv \frac{1}{m_2} \mod m_1$$

Dann $x = a_1 \cdot \underbrace{m_2 \cdot m_2'}_{1} + \underbrace{a_2 \cdot m_1 \cdot m_1'}_{\equiv 0} \mod m_1$

$\equiv a_1 \mod m_1$

Beispiel:

$$x \equiv 1 \mod 2 \qquad a_1 = 1,\ m_1 = 2$$
$$x \equiv 2 \mod 3 \qquad a_2 = 2,\ m_2 = 3$$

$$\Rightarrow x = a_1 \cdot m_2 \cdot m_2' + a_2 \cdot m_1 \cdot m_1'$$
$$1 \cdot 3 \cdot 1 + 2 \cdot 2 \cdot 2 \equiv 11 \mod 6$$
$$\equiv 5 \mod 6$$

$$m_2' \equiv \frac{1}{m_2} \mod m_1$$
$$\equiv \frac{1}{3} \mod 2 \equiv \frac{1}{1} \mod 2 \equiv 1 \mod 2$$

$$m_1' \equiv \frac{1}{2} \bmod 3 \equiv \frac{1}{-1} \bmod 3 \equiv -1 \equiv 2 \bmod 3$$

Lösung:

$$x = a_1 \cdot m_2 \cdot m_2' + a_2 \cdot m_1 \cdot m_1' \bmod (m_1 \cdot m_2)$$

$$m_1' \equiv \frac{1}{m_1} \bmod m_2 \qquad m_2' \equiv \frac{1}{m_2} \bmod m_1$$

weitere Übung:

$$x \equiv 5 \mod 6$$
$$x \equiv 2 \mod 5$$
$$x = 5 \cdot 5 \cdot 5 + 2 \cdot 6 \cdot 1 = 137 \equiv 17 \mod 30$$

Teilproblem: Dividieren mod m

$$\frac{a}{b} \mod m$$
$$\equiv a \cdot \left(\frac{1}{b}\right) \mod m$$

$x = \frac{1}{b} \mod m$ berechnen, $m \in \mathbb{N}$, $ggT(b,m) = 1$

$b \cdot x \equiv 1 \mod m$

$m \mid (b \cdot x - 1)$

$$\exists y \in \mathbb{Z}, \quad m \cdot y = b \cdot x - 1 \iff \underbrace{bx - my}_{\text{erweiterter Euklidischer Algorithmus}} = \boxed{1}^{\,ggT(b,m)}$$

Erweiterter Euklidischer Algorithmus

$1 = \underset{x}{8} \cdot 31 - \underset{y}{13} \cdot 19$

ursprünglicher Euklid: Div mit Rest

$b = 19 \quad a = 31$

$31 = \underline{1} \cdot 19 + \boxed{12}$

$19 = \underline{1} \cdot 12 + \boxed{7}$

$12 = 1 \cdot 7 + \boxed{5}$

$7 = 1 \cdot 5 + \boxed{2}$

$5 = 2 \cdot 2 + 1 \longrightarrow 1 = 5 - 2 \cdot 2$

$1 = 5 - 2 \cdot (7 - 1 \cdot 5)$

$1 = 3 \cdot 5 - 2 \cdot 7$

$1 = 3 \cdot (12 - 1 \cdot 7) - 2 \cdot 7$

$1 = 3 \cdot 12 - 5 \cdot 7$

$1 = 3 \cdot 12 - 5 \cdot (19 - 1 \cdot 12)$

$1 = 8 \cdot 12 - 5 \cdot 19$

Übung:

Erweiterter Euklid: $a = 43$, $b = 31$

$$a \cdot x + b \cdot y = 1$$