Weitere Attacken gegen Diffie-Hellman

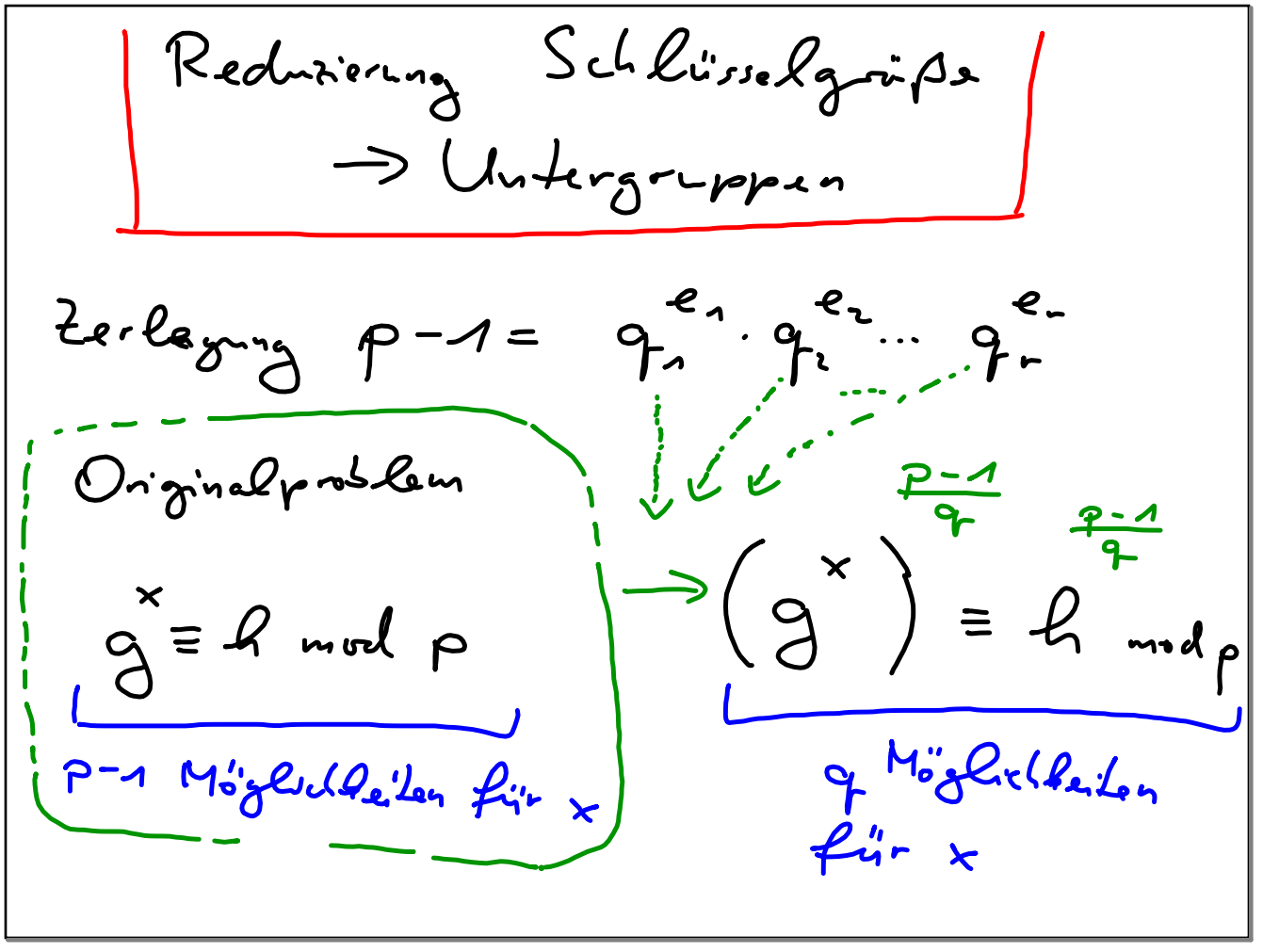
(Shanks: baby-step giant-step Speicherplatzverbrauch

falls $p \approx 10^{50}$

$\rightarrow$ Hashtabelle $\approx \sqrt{10^{50}} = 10^{25}$

10^{13} TB , 10^{10} PB)

- Reduzierung der Schlüsselgröße
- Hashtabelle vermeiden


Reduzierung Schlüsselgröße
→ Untergruppen
Zerlegung $p-1 = q_1^{e_1} \cdot q_2^{e_2} \cdots q_r^{e_r}$
Originalproblem
$g^x \equiv h \bmod p$
$p-1$ Möglichkeiten für x
$\frac{p-1}{q}$
$\frac{p-1}{q}$
$(g^x) \equiv h \bmod p$
q Möglichkeiten für x

Beispiel:

$$2^x \equiv 6 \mod 11$$

$p = 11, \quad p-1 = 10 = 2 \cdot 5$

$q_1 = 2, \quad q_2 = 5$

$q = 2$:

$$\left(2^x\right)^{\frac{11-1}{2}} \equiv 6^{\frac{11-1}{2}} \mod 11$$

$$\left(2^5\right)^x \equiv 6^5 \mod 11 \Leftrightarrow 10^x \equiv 10 \mod 11$$

$x \equiv 1 \mod 2$

$q = 5$:

$$\left(2^x\right)^{\frac{11-1}{5}} \equiv 6^{\frac{11-1}{5}} \mod 11$$

$$\left(2^2\right)^x \equiv 6^2 \mod 11$$

$$4^x \equiv 3 \mod 11$$

für x gibt es $q=5$ Mögl.

$\rightarrow x \equiv 4 \mod 5$

Teilergebnisse:

$p = 11, p - 1 = 10 = 2 \cdot 5$

$$x \equiv 1 \mod 2$$
$$x \equiv 4 \mod 5$$

$x = 9, 19, 29, \ldots$

$x \equiv 9 \mod 10$

Chinesischer Restsatz

↳ hat effiziente Lösung

Einschub: Lösung für chin. Restsatz

(chinese remainder theorem, CRT)

$$x \equiv a_1 \bmod m_1$$
$$x \equiv a_2 \bmod m_2$$

$ggT(m_1, m_2) = 1$

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

$x \bmod m_1$: $a_1 \cdot m_2 \cdot m_2' \equiv a_1 \cdot 1 = a_1 \bmod m_1$

$x \bmod m_2$: $a_2 \cdot m_1 \cdot m_1' \equiv a_2 \cdot 1 = a_2 \bmod m_2$

m_1' soll mod m_2 zu

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

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

ebenso:

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

Fortführung des Beispiels:

$$x \equiv 1 \mod 2 \quad | \quad a_1 = 1, m_1 = 2$$
$$x \equiv 4 \mod 5 \quad | \quad a_2 = 4, m_2 = 5$$

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

$$m_1' \equiv \frac{1}{2} \mod 5 \;, \quad m_2' \equiv \frac{1}{5} \mod 2$$
$$m_1' \equiv 3 \mod 5 \;, \quad m_2' \equiv 1 \mod 2$$

$$x = a_1 \cdot m_2 \cdot m_2' + a_2 \cdot m_1 \cdot m_1'$$
$$= 1 \cdot 5 \cdot 1 + 4 \cdot 2 \cdot 3 = \boxed{29 \equiv 9 \mod 10}$$

$\Rightarrow x = 9$ ist Lösung des CRT-Problems

Pollard: Zahlenfolge statt Hashtabelle

Gegeben ist ein Problem der Form

$$g^x = h$$

x mit q möglichen Werten

g, h gegeben

x mod q gesucht

---

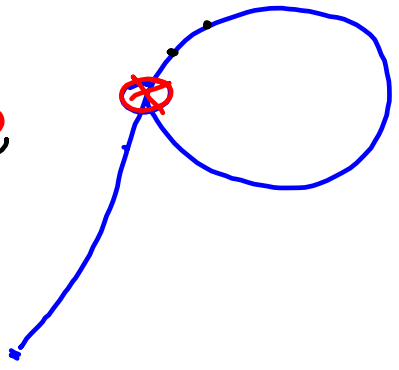
es werden Zahlen der Form $g^k \cdot h^\ell$

ausgerechnet

irgendwann wird eine berechnet*

die schon einmal berechnet* war ⊗,

danach wiederholt sich die Folge



$$g^k \cdot h^\ell = g^{k'} \cdot h^{\ell'}$$

(*) (*)

$$\Rightarrow g^k \cdot (g^x)^\ell = g^{k'} \cdot (g^x)^{\ell'}$$

$$\Rightarrow k + x \cdot \ell \equiv k' + x\ell' \mod q$$

$$\Rightarrow x \equiv \frac{k - k'}{\ell' - \ell} \mod q$$

Beispiel:

$g = 5, \quad h = 12, \quad p = 23, \quad q = 11$

$5^x \equiv 12 \mod 23, \quad p - 1 = 2 \cdot 11$

$q = 2$ $\qquad$ $q = 11$

$(5^x)^{\frac{23-1}{2}} \equiv 12^{\frac{23-1}{2}} \mod 23$

$(5^x)^{\frac{23-1}{11}} \equiv (12)^{\frac{23-1}{11}} \mod 23$

$(5^2)^x \equiv 12^2 \mod 23$

$\boxed{2^x \equiv 6 \mod 23}$

Pollard

$$2^x \equiv 6 \mod 23$$

Zahlenfolge:

$$y_0 \equiv g \cdot h \equiv g^1 \cdot h^1 \mod p$$

$$y_{i+1} \equiv \begin{cases} g \cdot y_i \mod p & \text{falls } y_i \equiv 0 \mod 3 \\ h \cdot y_i \mod p & \text{falls } y_i \equiv 1 \mod 3 \\ y_i^2 \mod p & \text{falls } y_i \equiv 2 \mod 3 \end{cases}$$

im Beispiel:

$$y_0 \equiv g \cdot h \equiv 2 \cdot 6 \equiv \boxed{12} \mod 23$$

$$y_1 \equiv g \cdot y_0 \equiv 2 \cdot 12 \equiv 1 \mod 23$$

$$y_2 \equiv h \cdot y_1 \equiv 6 \cdot 1 \equiv 6 \mod 23$$

$$y_3 \equiv g \cdot y_2 \equiv 2 \cdot 6 \equiv \boxed{12} \mod 23$$

k	ℓ
1	1
2	1
2	2
3	2

$$g^1 \cdot h^1 \equiv \square \equiv \square \equiv g^3 \cdot h^2 \mod p$$

$$x \equiv \frac{k - k'}{\ell' - \ell} \mod q$$

$$\equiv \frac{1-3}{2-1} \mod 11 \equiv \frac{-2}{1} \equiv -2 \mod 11$$

$$\Rightarrow x \equiv 9 \mod 11$$

Übung:

1) $x \bmod 2$

2) $x \bmod 2 \;/\; x \bmod 11$

$\longrightarrow x \bmod 22$