# Pohlig-Hellman (1)

$$a^x \equiv_q b \;\Leftrightarrow\; \log_a b \equiv_q x \;\;,\;\; q \;is\; prime$$
$$a \;\; is\; generator\,,\;\; that\; is \;\; ord(a) = q-1 = n \Rightarrow a^n \equiv_q 1$$
$$n = \prod p_i^{\lambda_i} = p_1^{\lambda_1} * \ldots * p_t^{\lambda_t}$$

Chinese Remainder Theorem

$$z_1 \equiv x \;\; (mod\; p_1^{\lambda_1})$$
$$\ldots$$
$$z_t \equiv x \;\; (mod\; p_t^{\lambda_t})$$

$$z = z_i\,,\;\; p = p_i\,,\;\; \lambda = \lambda_i \;\; (Simplifying\; the\; notation)$$

$$z = z_0 + z_1 p + z_2 p^2 + \ldots + z_{\lambda-1} p^{\lambda-1}$$
$$with \;\; z \in \{0,1\,,\ldots,\,p-1\}\,(p-adic\;\; representation\;\; of\;\; z)$$

$$c \equiv_q a^{\frac{n}{p}} \;\Rightarrow\; c^p \equiv_q a^n \equiv_q 1 \;\Rightarrow\; ord(c) = p$$
$$a^{x*\frac{n}{p}} \equiv_q b^{\frac{n}{p}} \equiv_q c^x$$
$$c^x \equiv_q c^z \equiv_q c^{z_0 + z_1 p + z_2 p^2 + \ldots + z_{\lambda-1} p^{\lambda-1}}$$
$$c^x \equiv_q c^{z_0} * c^{z_1 p} * c^{z_2 p^2} * \ldots * c^{z_{\lambda-1} p^{\lambda-1}}$$
$$ord(c) = p \;\Rightarrow\; c^x \equiv_q c^{z_0}$$
$$b^{\frac{n}{p}} \equiv_q c^{z_0}$$
$$(Subordinate\; DL-problem\,,\; compute \;\; z_0 \;\; with\; BSGS)$$

# Pohlig-Hellman (2)

*Assume that for a* $j \leq \lambda - 1$ *the coefficients* $z_0, z_1, \ldots, z_{j-1}$ *are already computed.*
*Then we can calculate the group element* $b_j$ *with*

$$b_j \equiv_q \left(\frac{b}{a^{z_0 + z_1 p + \ldots + z_{j-1} p^{j-1}}}\right)^{\frac{n}{p^{j+1}}}$$

$$a^{x * \frac{n}{p^{j+1}}} \equiv_q b^{\frac{n}{p^{j+1}}} \equiv_q a^{z * \frac{n}{p^{j+1}}}$$

$$b_j \equiv_q \frac{a^{z * \frac{n}{p^{j+1}}}}{a^{\frac{(z_0 + z_1 p + \ldots + z_{j-1} p^{j-1}) * n}{p^{j+1}}}}$$

$$b_j \equiv_q \frac{a^{\frac{(z_0 + z_1 p + z_2 p^2 + \ldots + z_{\lambda-1} p^{\lambda-1}) * n}{p^{j+1}}}}{a^{\frac{(z_0 + z_1 p + \ldots + z_{j-1} p^{j-1}) * n}{p^{j+1}}}}$$

$$b_j \equiv_q a^{\frac{(z_j p^j + z_{j+1} p^{j+1} + \ldots + z_{\lambda-1} p^{\lambda-1}) * n}{p^{j+1}}}$$

$$b_j \equiv_q a^{z_j \frac{n}{p} + z_{j+1} n + \ldots + z_{\lambda-1} p^{\lambda-j-2} n}$$

$$b_j \equiv_q a^{z_j \frac{n}{p}} * a^{z_{j+1} n} * \ldots * a^{z_{\lambda-1} p^{\lambda-j-2} n}$$

$$ord(a) = n \Rightarrow b_j \equiv_q a^{z_j \frac{n}{p}} \equiv_q c^{z_j}$$

$$(\text{Subordinate DL} - \text{problem, compute } z_j \text{ with BSGS})$$