NOTES ON THE POHLIG-HELLMAN ATTACK ON THE DISCRETE LOG PROBLEM

Let $p =$ large prime and $1 < \alpha < p$ a primitive root (mod p). If α, β, p are known and

$$\alpha^x \equiv \beta \pmod{p},$$

the Discrete Log Problem (DLP) is to find x with $1 < x < p$.

Solving DLP with a brute force attack of R tries: *Let's assume we know the solution x is not too big. For example assume we know $1 \le x < R$ for some small integer R. Then we simply compute*

$$\alpha^0 \equiv 1 \,(\text{mod } p),\ \ \alpha \,(\text{mod } p),\ \ \alpha^2 \,(\text{mod } p),\ \ \alpha^3 \,(\text{mod } p),\qquad \ldots,\qquad ,\alpha^{R-1} \,(\text{mod } p).$$

One of the above R numbers has to equal to β. Then we have found x.

Finding $x \,(\text{mod } q)$ with the Pohlig-Hellman attack:

Step 1: Find a small integer q where q divides $p-1$.

Step 2: Compute $A = \alpha^{\frac{p-1}{q}} \,(\text{mod } p)$.

Step 3: Compute $B = \beta^{\frac{p-1}{q}} \,(\text{mod } p)$.

Step 4: Solve $A^y \equiv B \,(\text{mod } p)$ with a brute force attack of q tries. Then $y \equiv x \pmod{q}$.

Example: Consider the Discrete Log Problem: $2^x \equiv 17 \,(\text{mod } 61)$. Find $x \,(\text{mod } 5)$.

Step 1: $5 \mid (61-1)$.

Step 2: $A \equiv 2^{12} \pmod{61} = 9$.

Step 3: $B \equiv 17^{12} \pmod{61} = 20$.

Step 4: We make 5 tries in trying to solve $9^y \equiv 20 \pmod{61}$:

$9^0 \equiv 1 \pmod{61},\ 9^1 \equiv 9 \pmod{61},\ 9^2 \equiv 20 \pmod{61},\ 9^3 \equiv 58 \pmod{61},\ 9^4 \equiv 34 \pmod{61}.$

We see that $y = 2$ is the solution. So $x \equiv 2 \pmod{5}$. Actually $x = 47$ is the solution.

Why does this work? The Pohlig-Hellman attack works because

$$\alpha^x \equiv \beta \pmod{p} \quad\Longrightarrow\quad \alpha^{x\cdot\frac{p-1}{q}} \equiv \beta^{\frac{p-1}{q}} \pmod{p} \quad\Longrightarrow\quad \alpha^{y\cdot\frac{p-1}{q}} \equiv \beta^{\frac{p-1}{q}} \pmod{p},$$

where $y \equiv x \pmod{q}$.

Finding x with the Pohlig-Hellman attack:

If one finds $x \pmod{q}$ for sufficiently many coprime integers q then one may solve for x using the Chinese Remainder Theorem.