# The Pohlig-Hellman Algorithm

Let $G$ be a group and $g \in G$ of order $N$, where $N = q_1^{e_1} q_2^{e_2} \cdots q_k^{e_k}$ is the prime factorization

The following algorithm solves the DLP $g^x = h$

1. Create $k$ DLPs, one for each prime factor of $N$:

   $$\text{Let } N_1 = \frac{N}{q_1^{e_1}}, \quad g_1 = g^{N_1}, \quad h_1 = h^{N_1} \quad \text{then} \quad g_1^{y_1} = h_1,$$

   $$\text{Let } N_2 = \frac{N}{q_2^{e_2}}, \quad g_2 = g^{N_2}, \quad h_2 = h^{N_2} \quad \text{then} \quad g_2^{y_2} = h_2, \qquad \text{etc.}$$

2. Use your favorite method to solve these $k$ DLPs, giving solutions $\{y_1, y_2, \ldots, y_k\}$
3. Use the Chinese Remainder Theorem to find a solution $x$ to the system of equations

   $$x \equiv y_1 \mod q_1^{e_1}, \quad x \equiv y_2 \mod q_2^{e_2}, \quad \ldots \quad x \equiv y_k \mod q_k^{e_k}$$

4. $x$ is a solution to the original DLP $g^x = h$

# The Mathematica notebook posted for today might be useful

1. Solve $5^x \equiv 7983 \mod 8017$ using the Pohlig-Hellman algorithm.

2. Solve the DLP $10^x \equiv 55280118052309167960656295593012 \mod 129003898576076751531908549775811$

   Notice this is the problem from class on Feb 5

3. (a) If you were to apply Pollard's $\rho$ to problem #2 directly, what is the expected number of steps before you obtain a collision?

   (b) If you were to apply Shanks to problem #2 directly, how long is each list? How many terabytes would it take to hold the two lists?