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:

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

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

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 will be quite useful

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

2. Consider the DLP $g^x \equiv h \mod p$ where

   $$g = 10, h = 5061310631921860520186653893981 8, p = 1290038985760767515319085497 75811$$

   (a) Consider applying Shank's Babystep-Giantstep algorithm to this DLP directly.
      (i) How long would each list be?
      (ii) How many digits are in the binary expansion of p?
      (iii) How many bytes are required to store each integer in the lists?
      (iv) How many terabytes are required to store each list?
      Let's not use Shank's directly, ok?

   (b) Solve the DLP using the Pohlig-Hellman algorithm with Shank's to solve the smaller DLPs.

      What is the longest list you create when applying Shank's in your solution?