

The *Pohlig-Hellman attack* works in any group and is a way to break the DLP in the full group by breaking the DLP in subgroups of prime order. In particular you'll see in the exercise that it works against the DLP in \mathbb{F}_{1013}^* by solving DLPs in groups of size 2, 11, and 23. Here is the general description:

Let G be a cyclic group generated by g and let the challenge be to find $\log_g h = a$. Let the group order n factor as $n = \prod_{i=1}^r p_i^{e_i}$ where $p_i \neq p_j$ for $i \neq j$ and $e_i \in \mathbb{Z}_{>0}$. Then a can be computed from the information

$$\begin{aligned} a &\equiv a_1 \pmod{p_1^{e_1}} \\ a &\equiv a_2 \pmod{p_2^{e_2}} \\ a &\equiv a_3 \pmod{p_3^{e_3}} \\ &\vdots \\ a &\equiv a_r \pmod{p_r^{e_r}} \end{aligned}$$

by using the Chinese remainder theorem. This is because the $p_i^{e_i}$ are coprime and their product is n . So, if one can find the DL modulo all $p_i^{e_i}$ one can compute the entire DL.

Put $n_i = n/p_i^{e_i}$. Since g has order n the element $g_i = g^{n_i}$ has order $p_i^{e_i}$. The element $h_i = h^{n_i}$ is in the subgroup generated by g_i and it holds that $h_i = g_i^{a_i}$, where $a_i \equiv a \pmod{p_i^{e_i}}$.

E.g. $\mathbb{F}_{16}^* = \langle g \rangle$ has 15 elements, so one can first solve the DLP $h = g^a$ modulo 3 and then modulo 5. For such small numbers one can simply compute h^5 and compare it to $1, g^5$, and g^{10} to find whether a is equivalent to 0, 1, or 2 modulo 3. Then one compares h^3 to $1, g^3, g^6, g^9$, and g^{12} to see whether a is congruent to 0, 1, 2, 3, or 4 modulo 5.

The same approach works also for \mathbb{F}_{17}^* which has $16 = 2^4$ elements, but the above doesn't do anything to help us solve the problem – it's the same 16 candidates.

Actually, in this case we can do much better! Write $a = a_0 + a_1 2 + a_2 2^2 + a_3 2^3$. Then h^8 is either equal to 1 or to $-1 = g^8$ depending on whether a_0 is 0 or 1. Once that result is known we can compare $(h/g^{a_0})^4$ with 1 and -1 to find a_1 etc. So we can solve a much smaller DLP 4 times (and some updating of the target). Note that only the h side needs to be updated, the g side remains the same ± 1 for all steps.

In general, instead of going for a modulo $p_i^{e_i}$ at once we can first obtain a modulo p_i , then update the target h to h/g^{a_0} and determine a modulo p_i^2 by comparing to the same powers of g as in the first step; then reduce modulo p_i^3 , etc. till $p_i^{e_i}$ by each time solving a DLP in a group of size p_i .

Here are the steps written as an algorithm. For each p_i in the factorization of n one does the following:

1. Put $h' = h$, $a_{i,-1} = 0$
2. for $j = 0$ to $e_i - 1$
 - (a) put $h' = h' / (g^{a_{i,j-1} p_i^{j-1}})$ //using precomputed g^{-1}
 - (b) solve the DLP of order p_i for $a_{i,j} = \log_{g^{n/p_i}}(h')^{n/p_i^{j+1}}$.

and then combine the $a_{i,j}$ to $a_i = \sum_{j=0}^{e_i-1} a_{i,j} p_i^j$ and then those $a_i \pmod{p_i^{e_i}}$ (using CRT) to $a \pmod{n}$.

Important: the Pohlig-Hellman attack handles one prime at a time, not a prime power. That means that your DL table has only p_i elements and that you solve e_i DLs in subgroups of order p_i . You can see the difference in the example with \mathbb{F}_{17}^* below.

Numerical examples:

$\mathbb{F}_{11}^* = \langle 2 \rangle$, find a so that $3 = 2^a$. So $g = 2$ and $h = 3$. Compute $n_1 = 10/2 = 5$, $g^{n_1} = 2^5 = -1$, and $h^{n_1} = 3^5 = 1$ to see that $a \equiv 0 \pmod{2}$. Then compute $n_2 = 10/5 = 2$, $g^{n_2} = 2^2 = 4$, $g^{2n_2} = 2^4 = 5$, $g^{3n_2} = 2^6 = 9$, and $g^{4n_2} = 2^8 = 3$ and compare that to $h^{n_2} = 3^2 = 9$ to see that $a \equiv 3 \pmod{5}$. These two congruences imply that $a = 8$ and indeed $g^8 = h$.

$\mathbb{F}_{17}^* = \langle 3 \rangle$, find a so that $7 = 3^a$. So $g = 3$ and $h = 7$. We will also need $g^{-1} = 6$. In this example we will obtain a one bit at a time. First compare $h^8 = 7^8 = -1$ to 1 and -1 to see that $a \equiv 1 \pmod{2}$. Then compute $h' = h/g = 7 \cdot 6 = 8$ and then $(h')^4 = -1$, so also the next bit is 1. Then compute the update on h' as $h'/g^2 = 8 \cdot 6^2 = 16$. Then $(h')^2 = 1$ to see that the next bit is 0, so $a \equiv 3 \pmod{8}$ and we don't need to update h' .

Finally, since $h' = 16 = -1$ we see that the highest bit is 1, so $a \equiv 1 + 2 + 8 = 11 \pmod{16}$ and indeed $3^{11} = 7$. This solved the DLP in \mathbb{F}_{17}^* with just 4 very easy computations and comparisons. So computing DLs in fields \mathbb{F}_p with $p = 2^r + 1$ is easy.