Cryptology, homework sheet 6

Due 26 October 2021, 13:15

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually.
For this exercise you can use Sage for computations in the finite field. You may not use the built-in function for solving the DLP but follow the algorithm specified.

1. This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ for some prime p. Let $p = 1249$ and note that $p - 1 = 2^5 \cdot 3 \cdot 13$. A generator of $\mathbb{F}_p^*$ is $g = 7$. Bob's public key is $h_b = g^b = 1195$.

   Use the Pohlig-Hellman attack to compute Bob's secret key b; make sure to handle each power of 2 separately as in the algorithm description.

   Verify your answer, i.e., compute g^b. | 10 points