Cryptology, homework sheet 2

Due 28 September 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 compuations on the elliptic curve. You may not use the built-in function for solving the DLP but follow the algorithm specified.

1. Verify that $P = (237, 122)$ and $Q = (56, 366)$ are on the curve $E : y^2 = x^3 + x + 2$ over $\mathbb{F}_{409}$.
   Solve the DLP to compute $a = \log_P Q$ using the Pohlig–Hellman method.
   Make sure to treat prime powers p^e the correct way, i.e. by solving e DLPs in the subgroup of size p.
   For the DLP of size 53 use the BSGS algorithm. | 10 points |