Cryptology, homework sheet 4

Due 03 Octobber 2023, 13:30

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually.

1. For this exercise you may (and should) use a computer algebra system like sage for doing the elliptic curve computations. You need to hand in your sage code, i.e. anything you typed, as part of your solution.

   The elliptic curve
   $$y^2 = x^3 + x + 20 \text{ over } \mathbb{F}_{41}$$
   has 53 points. The point $P = (3, 38)$ has order 53. The point $P_A = (25, 34)$ is a multiple of P. Use Pollard's rho method **with Floyd's cyle-finding algorithm** to compute the discrete logarithm $a = \log_P(P_A)$ of P_A with base P.

   We use starting point $W_0 = S_0 = F_0 = 2P + 3P_A$ and a very small set of precomputed points $R_0 = 23P + 13P_A, R_1 = 19P + 11P_A, R_2 = 2P + 41P_A$, and $P_3 = 25P + 37P_A$ so that the step function is defined by adding R_i where $i \equiv x(W) \bmod 4$, where $x(W)$ is considered as an intger in $[0, 40]$.

   Verify your result.
   Each point that you compare should be stated, i.e., all S_i and F_i, but make sure to only compare F and S at the same index.
   You do not need to document the arihmetic steps taken in computing the elliptic-curve additions, but you do need to documnet the verification. | 15 points |