Cryptology, homework sheet 4

Due 24 September 2024, 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 $W_0 = 2P + 3P_A$ and define the"random"wllk by t4aking a very small set of precomputed points $R_0 = 23P + 13P_A, R_1 = 19P + 11P_A, R_2 = 2P + 41P_A$, and $P_3 = 25P + 37P_A$ and computing steps $W_{i+1} = W_i + R_j$, where j is chosen using the x-coordinate of the current point W_i, i.e., $j \equiv x(W_i) \bmod 4$, where $x(W_i)$ is considered as an intger in $[0, 40]$.

   For Floyd's method you do a fast walk $F_i = W_{2i}$ and a slow walk $S_i = W_i$, both starting at $W_0 = S_0 = F_0$.

   Note that at the begining we know W_0 as a combination of P and P_A and that at every step we add a known combination of these points, so for each step we know the b and c from the lecture and thus can compute the DLP once we find a collision.

   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 (field addition, multiplication, division) taken in computing the elliptic-curve additions, but you do need to documnet the verification. | 15 points |