Cryptology, homework sheet 3

Due 29 September 2022, 10:30

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

1. The elliptic curve
$$y^2 = x^3 + x + 3 \text{ over } \mathbb{F}_{43}$$
has 47 points. The point $P = (19, 42)$ has order 47. The point $P_A = (28, 15)$ is a multiple of P.

   (a) Use the BSGS method to compute the discrete logarithm $a = \log_P(P_A)$ of P_A with base P.
   Verify your result.
   Each point that you compute should be documented, i.e., all baby steps and all the giant steps until you find a match. You do not need to document the arihmetic steps taken in computing the elliptic-curve additions. [5 points]

   (b) Use the schoolbook version of Pollard rho and Floyd's cycle-finding algorithm to solve this DLP using starting point $S_0 = F_0 = W_0 = 5P_A = (36, 30)$ and the step function
$$W \leftarrow \begin{cases} W + P \\ W + P_A \\ 2W \end{cases}, b \leftarrow \begin{cases} b + 1 \\ b \\ 2b \end{cases}, c \leftarrow \begin{cases} c \\ c + 1 \\ 2c \end{cases}, \text{ for } s(W) = \begin{cases} 0 \\ 1 \\ 2 \end{cases}.$$
   Here $s(W)$ takes the integer representation of $x(W)$ in $[0, 42]$ and outputs the remainder of division by 3.
   Keep a tally of the values of b and c so that you know at any moment which coefficients you need to use to get to that point, starting with $b = 0, c = 5$ for the starting point.
   Each point that you compute should be documented, i.e. all the slow steps and all the fast steps until you find a match of $S_i = F_i$. You do not need to document the arihmetic steps taken in computing the elliptic-curve additions. You will likely find it easiest to write out all steps you're taking, but make sure only to compare points at the same i. [10 points]