Cryptography, exercise sheet 4 for 22 Sep 2026

1. Copy from last week:

   Use the schoolbook version of Pollard rho and Floyd's cycle-finding algorithm to solve the DLP from exercise 5 last week using starting point $S_0 = F_0 = W_0 = 5P_A = (36, 30)$ and the step function

$$W \leftarrow \begin{cases} W + P \\ W + P_A \\ 2W \end{cases}, \quad b \leftarrow \begin{cases} b + 1 \\ b \\ 2b \end{cases}, \quad c \leftarrow \begin{cases} c \\ c + 1 \\ 2c \end{cases}, \text{ for } s(W) = \begin{cases} 0 \\ 1 \\ 2 \end{cases}.$$

   As a reminder, the curve is $y^2 = x^3 + x + 3$ over $\mathbb{F}_{43}$ with 47 points. The base point $P = (19, 42)$ has order 47, the target point is $P_A = (28, 15)$.

2. Discuss how you can document the work you did in exercise 1 so that one can follow the steps you did to grade it (think of how partial credit could be awarded should you get a wrong result because of a small calculation error or should you run out of time).

3. Let $p = 1000003$. The elliptic curve $E : y^2 = x^3 - x$ over $\mathbb{F}_p$ has $1000004 = 2^2 \cdot 53^2 \cdot 89$ points. $P = (101384, 614510)$ is a point of order $2 \cdot 53^2 \cdot 89$ and $Q = aP = (670366, 740819)$ is a multiple of P.

   (a) Show that the point $P_{53} = (2 \cdot 53 \cdot 89)P$ has order 53.

   (b) Compute $a_2 \equiv a \bmod 2$ by solving the DLP in the order-2 subgroup.

   (c) Use the BSGS algorithm on P_{53} and $(2 \cdot 53 \cdot 89)Q$ to compute $a \bmod 53$.

   (d) Then use the BSGS algorithm *with the same baby steps* to solve the DLP in the order-53 subgroup to get a_3.
   Make sure to update Q before solving the second one – and do not overwrite your original Q.

   (e) Solve the DLP in the size-89 subgroup. Feel free to use a for loop in Sage to solve this or the built in Sage function, but make sure to compute S and R, the new base and target.

   (f) Use the Chinese remainder theorem to compute a. Test your solution.

4. Let point P have order 411672 and point P_A be a multiple of P. Explain how to compute the DLP of P_A base P using the Pohlig-Hellman attack, i.e., explain what computations you will do and which ones depend on previous partial results.