Cryptography, exercise sheet 4 for 26 Sep 2023

Some of these exercises are copied from sheet 3 because I didn't manage to cover all the material I wanted to cover on the 19th when we were locked out of our lecture room.

1. Write 20210914 in binary and compute the coefficients of the presentation with window width $w = 3$.

2. Test your understanding of the Montgomery ladder by writing out the intermediate values for P_0 and P_1 encountered in comuting $19P$. We did a small example in class for computing $5P$.

3. 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 $P_A = (28, 15)$.

4. Discuss how you can document the work you did in exercise 3 so that one can grade it.

5. 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 $P_A = aP = (670366, 740819)$ is a multiple of P.

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

   (b) Use the BSGS algorithm to compute $a \bmod 53$ in the subgroup of order 53.