Cryptography, exercise sheet 4 for 26 Sep 2024

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. Explain to one of your team mates or one of the TAs the hash collision conundrum that one cannot define a formal notion of security for fixed hash functions (as opposed to members of a family).

4. **Multi-target attacks.** Sometimes an attacker gets to attack multiple targets at once and is satisfied breaking any *one* of them. For hash functions multi-target preimage attacks are interesting. We speak of a t-target preimage attack if the attacker is given the outputs $h_k(m_1), h_k(m_2), \ldots, h_k(m_t)$ (and k) but not the inputs $m_1, m_2, \ldots, m_t$ of a hash function $h : \{0,1\}^n \times \{0,1\}^{\ell(n)} \to \{0,1\}^n$ and has the goal of finding a pair (i, x) such that $h_k(x) = h_k(m_i)$.

   (a) Show that a t-target preimage attack A succeeding with probability p can be turned into a 1-target preimage attack, i.e., a regular preimage attack, taking the same time as A and succeeding with probability p/t.
   Note that you need to ensure that the inputs to A are properly distributed and that you have no influence over which i the algorithm picks.

   (b) The algorithm you just developed is actually also a reduction. What did you prove with that algorithm (In terms of property X implies property Y)?

   (c) Find an attack that takes time $2^n/t$ to succeed in finding one (i, x) with high probability.

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

   (b) Use the BSGS algorithm on P_{53} and $(2 \cdot 53 \cdot 89)P_A$ to compute a mod 53.