Cryptology, homework sheet 4

Due 06 October 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.
For the first exercise you can use Sage for compuations on the elliptic curve. You may not use the built-in function for solving the DLP but follow the algorithm specified.

1. The points $P = (237, 122)$ and $Q = (56, 366)$ are on the curve $E : y^2 = x^3 + x + 2$ over $\mathbb{F}_{409}$. The point P has order $2^3 \cdot 53$.
   Solve the DLP to compute $a = \log_P Q$ using the Pohlig–Hellman method.
   Make sure to treat prime powers p^e the correct way, i.e. by solving e DLPs in the subgroup of size p.
   For the DLP of size 53 use the BSGS algorithm. | 11 points |

2. **Combination of hash functions.** Are the following claims true or false? Either present a proof by giving a reduction as in the lecture or a counter example.

   (a) Let $h : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be an efficient keyed permutation. Let $H = h \circ h$ be the permutation resulting from applying h twice with the same key, i.e., $H(k, m) = h(k, h(k, m))$.
   Claim: If h is preimage resistant (PRE), H is preimage resistant. | 2 points |

   (b) Let $h_1 : \{0,1\}^{n_1} \times \{0,1\}^{\ell(n_1)} \to \{0,1\}^{n_1}$ and $h_2 : \{0,1\}^{n_2} \times \{0,1\}^{n_1} \to \{0,1\}^{n_2}$ be hash functions.
   Claim: The combined hash function $H : \{0,1\}^{n_1+n_2} \times \{0,1\}^{\ell(n_1)} \mapsto \{0,1\}^{n_2}; (\langle k_1, k_2\rangle, m) \mapsto h_2(k_2, h_1(k_1, m))$ is collision resistant if at least one of h_1 and h_2 is collision resistant and h_2 is not constant.
   | 2 points |