Cryptology, homework sheet 4

Due 29 September 2026, 13:30

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

1. This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ for some prime p. Let $p = 1249$ and note that $p - 1 = 2^5 \cdot 3 \cdot 13$. A generator of $\mathbb{F}_p^*$ is $g = 7$. Bob's public key is $h_b = g^b = 1195$.

   Use the Pohlig-Hellman attack to compute Bob's secret key b; make sure to handle each power of 2 separately as in the algorithm description.

   Verify your answer, i.e., compute g^b. | 10 points |

2. A signature links the signer to a document in a way that anybody can check. Hence, signing uses the private key of the signer and verification uses the public key.

   The ElGamal signature scheme works as follows. Let $G = \langle P \rangle$ be a group of points of prime order ℓ and H be a hash function. User A picks a private key a and computes the matching public key $P_A = aP$. To sign message m, A picks a random $r \in (\mathbb{Z}/\ell)^*$, computes $R = rP$ and $R' \equiv x(R) \bmod \ell$, and computes $s \equiv r^{-1}(H(m) + R'a) \bmod \ell$. The signature is (R, s). Here $x(R)$ denotes the x-coordinate of the point R.

   The signature is verified by first computing $w_1 \equiv s^{-1}H(m) \bmod \ell, w_2 \equiv s^{-1}R' \bmod \ell$ and then checking that $w_1P + w_2P_A = R$.

   (a) Show that for a correctly generated signature indeed $w_1P + w_2P_A = R$ holds. | 1 point |

   (b) Alice publishes r along with her signature (R, s) and message m. Show how to obtain Alice's secret key a from this. | 2 points |

   (c) You obtain (R, s_1) on m_1 and (R, s_2) on m_2 (note, the same R, different m_i). Show how to obtain a. | 2 points |