Cryptology, homework sheet 5

Due 13 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.

1. The ElGamal signature scheme works as follows. Let $G = \langle P \rangle$ be a group of 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 nonce r, 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). The diffference to ECDSA is that we see the full point R, not just 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 $x(w_1P + w_2P_A) \equiv R' \bmod \ell$.

   (a) 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

   (b) You obtain (R_1, s_1) on m_1 and (R_2, s_2) on m_2 and know that these were generated such that $r_2 = r_1 + 1$.
   Show how to obtain a. 4 points

   (c) Show how evil Alice can pick her secret key a dependent on two fixed, given messages m_1 and m_2, so that she can later pretend that a signature (R, s) on m_1 was a signature on m_2. Note, this means *the same* signature (R, s) satisfies the verification equation for m_1 and m_2.
   State a as an expression in m_1, m_2, and the group order ℓ.
   Hint: You will also fix r for that signature now. 5 points

2. The lectures showed how TEA can be used to encrypt some input block b. Explain how decryption works, i.e., how to compute the input given the output and the key.
   Hint: Show how to invert one round and how to compose these steps.
   Hint: Looking at the diagram in lecture V can help. 4 points