Cryptology, homework sheet 3
Due 05 October 2021, 13:15

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

1. **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

2. The ElGamal signature scheme works as follows. Let $G = \langle P \rangle$ be a group of order ℓ. User A picks a private key a and computes the matching public key $Q = aP$. To sign message m, A picks a random nonce r, computes $R = rP$ and $R' \equiv x(R) \bmod \ell$, and computes $s \equiv r^{-1}(R' + H(m)a) \bmod \ell$. The signature is (R, s). This differs from ECDSA in that the full point R is sent in the first component.

   (a) 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. 3 points

   (b) You obtain (R_1, s_1) on m_1 and (R_3, s_3) on m_3 and know that these were generated not too long after one another using the same update by incrementing as above, such that $r_3 = r_1 + i$ for some small i. Show how to obtain i and a. 3 points