Cryptology, homework sheet 2
Due 19 September 2023, 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. **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. $\boxed{\text{2 points}}$

   (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.
   $\boxed{\text{2 points}}$

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 $w_1P + w_2P_A = R$.

   One thing to notice is that if r becomes known, then anybody can compute the private key a from the signature as $a \equiv (sr - H(m))/R' \bmod \ell$.

   (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. $\boxed{\text{2 points}}$

   (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. $\boxed{\text{4 points}}$

   (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. $\boxed{\text{5 points}}$