دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری

آزمون میانترم

مدرّس: دکتر شهرام خزائی

تاریخ: ۱۳۹۹/۸/۲۷

Problem 1

In all of the CPA-secure encryption schemes, the length of the ciphertext is greater than the length of the plaintext length. In this problem, we will show that this is necessary. Let $(\mathsf{Encrypt}, \mathsf{Decrypt})$ be a symmetric encryption scheme with message space $\{0,1\}^n$ and ciphertext space $\{0,1\}^m$.

1. Suppose that $n = m$. Show that $(\mathsf{Encrypt}, \mathsf{Decrypt})$ cannot be CPA-secure.
2. Suppose that $m = n + \ell$ for some $\ell < \frac{n}{2}$. Describe a CPA adversary that makes $O(2^{\ell/2})$ queries in the CPA-security game and distinguishes with constant probability. For simplicity (though not necessary), you may assume that for any choice of key k and message m, the output distribution of $\mathsf{Encrypt}(k, m)$ is uniform over a collection of up to 2^ℓ possible ciphertexts, where the distribution is over the encryption randomness. Be sure to fully describe your attack and give a precise analysis of the advantage (note that it suffices to lower bound the advantage by a constant).

Problem 2

Let $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}$ be a secure PRF. Use F to construct a function $F' : \{0,1\}^{\lambda+1} \times \{0,1\}^\lambda \to \{0,1\}$ with the following two properties:

- F' is a secure PRF.
- If the adversary learns the last bit of the key, then F' is no longer secure. You should (a) prove that F' is a secure PRF; and (b) describe an attack (and compute the advantage) when the adversary knows the last bit of the PRF key. This problem shows that leaking even a single bit of the secret key can break PRF security. **Hint:** Try changing the value of F at a single point.

Problem 3

Recall that in a Feistel system, we divide the state into left and right halves L_i, R_i and then define the new state by $L_{i+1} = R_i$ and $R_{i+1} = L_i \oplus f(K_i, R_i)$, where K_i is the key for the i-th round and f is a function of the key and half of the state. Prove that no matter what the function f is, the round transformation is 1-to-1, i.e., we can recover the old state from the new state and the key.

Problem 4

Let G be a PRG with expansion factor $\ell(n) > n$ and let $f : \{0,1\}^* \rightarrow \{0,1\}^*$ be a length-preserving bijection (i.e., a permutation) such that f is computable in deterministic polynomial time and define G' as follows:

$$G'(s) \coloneqq f(G(s))$$

Show that G' is also a PRG.

Problem 5

Consider the following message authentication code called BCMAC (for block cipher message authentication code") which is derived from a block cipher that operates on n-bit plaintexts. BCMAC takes as input a message M of bit length $2n-2$ and produces the corresponding tag as follows (here, E_K is encryption under the block cipher using key K and $||$ denotes concatenation):

1. Write $M = M_0||M_1$, where M_0, M_1 each have length $n-1$.
2. $BCMAC(M) \coloneqq E_K(0||M_0)||E_K(1||M_1)$

Show that BCMAC is not computation resistant as follows.
Suppose an adversary Eve has two distinct messages $M = M_0||M_1$ and $M' = M_0'||M_1'$, with $M_0 \neq M_0'$ and $M_1 \neq M_1'$, along with their respective message authentication tags $BCMAC(M)$ and $BCMAC(M')$. Carefully show how Eve can use this information to defeat computation resistance.
Hint: Computation resistant means Given zero or more message/MAC pairs, it is computationally infeasible to generate a new message/MAC pair where the message is distinct from all the given messages.