


دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری

آزمون میانترم

مدرّس: دکتر شهرام خزائی

تاریخ: ۱۳۹۹/۸/۲۷

Problem 1

Provide a formal definition for symmetric key encryption and CPA security.

Problem 2

Given a PRF F, construct a CPA-secure encryption scheme and prove its security.

Problem 3

Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{2\ell(n)}$ be a pseudo-random function. Consider the following cryptosystem Π over message space $\mathcal{M} = \{0,1\}^{\ell(n)}$

- $k \leftarrow \mathsf{Gen}(1^n)$: on input 1^n, output a random key k from $\{0,1\}^n$
- $\langle r, c\rangle \leftarrow \mathsf{Enc}_k(m)$: on input $k \in \{0,1\}^n$ and $m \in \{0,1\}^{\ell(n)}$, generate a random $r \in \{0,1\}^n$ and output

$$\langle r, c\rangle = \langle r, \text{expand}(m) \oplus f_k(r)\rangle$$

  where for every string $x \in \{0,1\}^*$ we define expand(x) as follows: replace each 0 in x with 00 and replace each 1 with 01 or 10 at random.

1. How does the decryption algorithm work? Hint: take care of $\perp$.
2. Is Π CPA-secure? If yes, prove your claim. If no, describe an attacker and compute its advantage.
3. Is Π CCA-secure? If yes, prove your claim. If no, describe an attacker and compute its advantage.

Problem 4

Let G_1, G_2 be two PRGs. Is G also a PRG? prove your answer.

$$G(s) \coloneqq G_1(s) \oplus G_2(0^{|s|})$$

Problem 5

Let F be a secure PRF. Prove that F' is also a secure PRF or show a PPT algorithm which breaks it.

$$F'(k, x) = F(k, x)||F(k, \bar{x})$$

where $\bar{x}$ is a bitwise negation of x.