


دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری

آزمون میانترم

مدرّس: دکتر شهرام خزائی

تاریخ: ۱۳۹۹/۹/۲۳

Problem 1

Give an example of a CPA-secure public-key encryption scheme where the ciphertexts are **not** pseudorandom, i.e. the ciphertexts are not indistinguishable from uniformly random strings.
Remark: This shows that CPA-security only says that the ciphertext hides the message; it does not mean that the ciphertexts look like random strings, and in many schemes, the ciphertext will not look like a random string.

Problem 2

Prove in the Random Oracle Model that $\mathsf{PRF}(k,x) := \mathsf{H}(k||x)$ is a secure PRF.

Problem 3

Say a public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ for n-bit messages is one-way if the probability $\Pr[\mathsf{PubK}^{\mathsf{ow}}_{\mathcal{A},\Pi}(n) = 1]$ is negligible for any PPT adversary $\mathcal{A}$. The experiment $\mathsf{PubK}^{\mathsf{ow}}_{\mathcal{A},\Pi}(n)$ is shown as follows.

- $\mathsf{Gen}(1^n)$ is run to obtain (pk, sk).
- A message m is chosen uniformly from $\{0,1\}^n$ and a ciphertext $c \leftarrow \mathsf{Enc}_{pk}(m)$ is generated.
- $\mathcal{A}$ is given (pk, c) and outputs m'.
- $\mathsf{PubK}^{\mathsf{ow}}_{\mathcal{A},\Pi}(n) = 1$ if $m' = m$.

1. Show that if a public-key encryption scheme Π for n-bit messages has CPA security, then Π is one-way.

2. Show that CPA security is strictly stronger than one-way security.
   Hint: Give a public-key encryption scheme example which has one-way security but does not have CPA security.

3. Construct a CPA secure KEM using one-way secure public-key encryption scheme in the random oracle model. Show your construction and proof ideas.