


دانشکده‌ی علوم ریاضی

رمزنگاری تحویل اصلی ۰۸ دی

تمرین : سری ۲

مدرّس : دکتر شهرام خزائی *تحویل نهایی ۱۵ دی*

- Upload your answers on courseware with the name: StudentNumber.pdf
- Upload a PDF file. Image and zip formats are not accepted.
- Similar answers will not be graded.
- NO answers will be accepted via e-mail.
- You should submit your answers before soft deadline.
- You will lose 5 percent for each day delay if you submit within a week after soft deadline.
- You can not submit any time after hard deadline.
- **One problem is optional.**
- For any question contact Ali Adibifar via @Aliadibifar.

Problem 1

Let F be a strong pseudorandom permutation, and define the following fixed-length encryption scheme: On input a message $m \in \{0,1\}^{n/2}$ and key $k \in \{0,1\}^n$, algorithm Enc chooses a uniform $r \in \{0,1\}^{n/2}$ and outputs the ciphertext $c := F_k(m||r)$. Prove that this scheme is CCA-secure.

Problem 2

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a secure PRF (i.e. a PRF where the key space, input space, and output space are all $\{0,1\}^n$). Which of the following is a secure PRF (there is more than one correct answer):

1. $$F'(k,x) = \begin{cases} F(k,x) & x \neq 0^n \\ 0^n & \text{otherwise} \end{cases}$$
2. $F'(k_1||k_2, x) = F(k_1, x) \oplus F(k_2, x)$
3. $F'(k,x) = F(k,x) \oplus 1^n$
4. $F'(k,x) = k \oplus x$

Problem 3

Let F be a length-preserving PRF and let $[k]_2^n$ denote the n-bit binary expression of the number k. Show that the following function is a PRG with expansion factor $n \to l \cdot n$

$$G(s) := F_s([1]_2^{|s|})||F_s([2]_2^{|s|})||\dots||F_s([l]_2^{|s|})$$

Problem 4

Suppose that $\{f_k : \{0,1\}^n \to \{0,1\}^n\}_{k \in \{0,1\}^n}$ is a family of pseudo-random functions. Consider an encyption system that its encryption algorithm is as follows:

$$Enc_k(m) = \begin{cases} (r, f_k(r) \oplus m, f_k(0^n)) & \text{if } m \neq f_k(0^n) \\ (r, f_k(r) \oplus m, k) & \text{if } m = f_k(0^n) \end{cases}$$

where r is randomly selected from n-bit strings. Show that this encryption system is multi-message secure but not CPA secure.

Problem 5

Consider the following keyed function F : For the security parameter n, the key is a matrix $A \in \mathrm{Mat}(n \times n, \mathbb{F}_2)$ and a vector $b \in \mathbb{F}_2^n$, where $\mathbb{F}_2$ denotes the field with 2 elements, i.e. $\mathbb{F}_2 = (\{0,1\}, \oplus, .)$ and $\mathbb{F}_2^n$ denotes the corresponding vector space of dimension n. Now we define $F_{A,b} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ by

$$F_{A,b}(x) = Ax + b$$

Decide whether F is a pseudorandom function and prove your answer.