


دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری تحویل اصلی: ۸ فروردین ۱۴۰۰

تمرین شماره ۲

مدرّس: دکتر شهرام خزائی *تحویل نهایی: ۱۵ فروردین ۱۴۰۰*

- 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 can't upload files bigger than 2 Mb, so you'd better type.
- Deadline time is always at 23:55 and will not be extended.
- 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.
- This problem set includes 55 points.
- For any question contact Aysan Nishaburi via `aysannishaburi@gmail.com`.

Problem 1

Let $\{p_k\}_{k\in\{0,1\}^*}$ be a pseudorandom permutation collection, where for $k \in \{0,1\}^n$, p_k is a permutation over $\{0,1\}^m$.

1. (10 Points) Consider the following encryption scheme (E, D) : $E_k(x) = p_k(x)$, $D_k(y) = p_k^{-1}(y)$. Prove that this scheme is not a CPA-secure encryption.
2. (10 Points) Consider the following scheme (E, D) that encrypts $m/2$-bit messages in the following way: on input $x \in \{0,1\}^{m/2}$, E_k chooses random $r \leftarrow_R \{0,1\}^{m/2}$ and outputs $p_k(x, r)$ (where comma denotes concatenation), on input $y \in \{0,1\}^m$, D_k computes $(x, r) = p_k^{-1}(y)$ and outputs x. Prove that (E, D) is a CPA-secure encryption scheme.

Problem 2

(25 Points) Suppose that $\{F_S : \{0,1\}^k \to \{0,1\}^k | S \in \{0,1\}^k\}$ is a pseudo-random family of functions from k-bit input to k-bit output, indexed by k-bit key ("seed"). We would like to get a new pseudo-random function family in which each function maps k bits to $2k$ bits. Consider the following construction, and for each show whether it is good or bad (namely whether the specified family is pseudo-random or not).

1. $F_S^1(x) = F_S(0^k)||F_S(x)$
2. $F_S^2(x) = F_S(x)||F_S(\bar{x})$
3. $F_S^3(x) = F_{0^k}(x)||F_S(x)$
4. $F_S^4(x) = F_{S_1}(x)||F_{S_2}(x)$,where $S_1 = F_S(0^k)$ and $S_2 = F_S(1^k)$

Problem 3

What is the output of an r-round Feistel network when the input is (L_0, R_0) in each of the following two cases:

1. (10 Points) Each round function outputs all 0's, regardless of the input.
2. (10 Points) Each round function is the identity function.