دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری تحویل اصلی: ۲۰ فروردین ۱۴۰۰

تمرین شماره ۳

مدرّس: دکتر شهرام خزائی *تحویل نهایی: ۲۷ 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 questions contact Elahe Kooshafar via `cyberian.eli@gmail.com`.

Problem 1

(15 points) Consider a symmetric encryption system that by receiving an n-bit message m, replaces each bit “0” of the message with bits “01” and each bit “1” with bits “00” or “11” at random, then encrypts the result with an $2n$-bit key using the OTP method. First explain the decryption algorithm and then show that this encryption system is not multi-message secure.

Problem 2

(20 points) 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:

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

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

Problem 3

(20 points) For a given PRG $G : S \to \{0,1\}^L$, and a given adversary $\mathcal{A}$, consider the following attack game:

- the adversary sends an index i, with $0 \leq i \leq L-1$, to the challenger.
- the challenger chooses a random s from S and computes $r = G(s)$ and sends $r[0], r[1], ..., r[i-1]$ to the adversary. ($r[i]$ is the i'th bit of r)
- the adversary outputs $g \in \{0,1\}$.

We say that $\mathcal{A}$ wins if $r[i] = g$, and we define $\mathcal{A}$'s advantage to be:

$$Adv^{\mathsf{Pre}}_{\mathcal{A},G} = |Pr[\mathcal{A}\ wins] - \frac{1}{2}|$$

We say that G is unpredictable if the value $Adv^{\mathsf{Pre}}_{\mathcal{A},G}$ is negligible for all p.p.t adversaries $\mathcal{A}$. Show that if G is secure, then it is unpredictable.