دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری	تحویل اصلی: ۳ آبان ۱۳۹۹
مدرّس: دکتر شهرام خزائی	تحویل نهایی: ۱۰ آبان ۱۳۹۹

تمرین شماره ۱

- 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 sets include 80 points.
- For any question contact Ghazal Khalighinejad via `ghazalkhn99@gmail.com`.

Problem 1

(20 Points) Let $G_1, G_2 : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ be two PRGs. Which of the following is a PRG (there is more than one correct answer):
Provide a proof or counter-example for your answers.

1. $G(k_1||k_2) = G_1(k_1) \oplus G_2(k_2)$ with $|k_1| = |k_2|$
2. $G(k) = G_1(0^{|k|})||G_2(k)$
3. $G(k) = G_1(k) \oplus G_2(k)$
4. $G(k) = G_1(G_2(k))$

Problem 2

(20 points) Suppose the message space of a symmetric key encryption system is infinite. (For example the set of natural numbers)
Prove or disprove that such a scheme can be perfectly secret.

Problem 3

(20 Points) We saw that any perfectly (and even imperfectly) secure private key encryption scheme needs to use a key as large as the message. But we actually made an implicit subtle assumption: that the encryption process is *deterministic*. In a *probabilistic encryption scheme*, the encryption function E may be probabilistic: that is, given a message x and a key k, the value $\mathsf{E}_k(x)$ is not fixed but is distributed according to some distribution $Y_{x,k}$. Of course, because the decryption function is only given the key k and not the internal randomness used by E, we need to require that $\mathsf{D}_k(y) = x$ for *every* y in the support of $Y_{k,x}$ (i.e., $\mathsf{D}_k(y) = x$ for every y such that $\Pr[\mathsf{E}_k(x) = y] > 0$). Prove that even a probabilistic encryption scheme cannot have key which is significantly shorter than the message. That is, show that for every probabilistic encryption scheme (D, E) using n-length keys and $(n+10)$-length messages, there exist two messages $x, x' \in \{0,1\}^{n+10}$ such that the distributions $\mathsf{E}_{U_n}(x)$ and $\mathsf{E}_{U_n}(x')$ are of statistical distance at least $1/10$.[1]

[1]**Hint:** Define $\mathcal{D}$ to be the following distribution over $\{0,1\}^{n+10}$: choose y at random from $\mathsf{E}_{U_n}(0^{n+5})$, choose k at random in $\{0,1\}^n$, and let $x = \mathsf{D}_k(y)$. Prove that if (E, D) is $1/10$-statistically indistinguishable then for every $x \in \{0,1\}^{n+10}$, $\Pr[\mathcal{D} = x] \geq 2^{-n-1}$. Derive from this a contradiction.

Problem 4

(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** $adv^{Pre}_{\mathcal{A},G}$ to be:

$$|\Pr[\mathcal{A} \text{ wins}] - \frac{1}{2}|$$

We say that G is ***unpredictable*** if the value of $adv^{Pre}_{\mathcal{A},G}$ is negligible for all p.p.t adversaries $\mathcal{A}$.

Show that if G is secure, then it is unpredictable