دانشکده‌ی علوم ریاضی

رمز نگاری		تحویل اصلی ۱۰ آذر
	تمرین : سری ۱	
مدرّس : دکتر شهرام خزائی		*تحویل نهایی ۱۷ آذر*

- 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.
- For any question contact Arash ashoori via @Arash0330.

Problem 1

Suppose X, Y are two probability distributions on the finite space Ω. The statistical distance between them is:

$$\Delta(X,Y) = \frac{1}{2}\sum_{w\in\Omega} |\Pr(X=w) - \Pr(Y=w)|$$

a) show this is a metric.
b) show that:

$$\Delta(X,Y) = \max_{A\subset\Omega} |\Pr(X\in A) - \Pr(Y\in A)|$$

c) Show that the most advantage possible for an attacker to distinguish between distributions X, Y equals $\Delta(X,Y)$.

Problem 2

a) Let M and K be arbitrary finite message and key spaces. Denote their sizes by $|M|$ and $|K|$, respectively. Show that there exists a symmetric key encryption system on these spaces such that the advantage of any attacker could not be more than
$\max(\frac{|M|}{|k|} - 1, 0)$.
b) Suppose the message space is $M = \{0,1\}^n$ and the key space is a subset of M with size $(1-\epsilon)2^n$ with a uniform distribution. Suppose the key encryption system is similar to the One Time Pad. Show that the advantage of any attacker can not be more than $\frac{\epsilon}{1-\epsilon}$, and also show for any $j \in \{1,2,..,n\}$ and $\epsilon = \frac{1}{2^j}$, there exists a key space as explained above and an attacker such that the advantege would be $\frac{\epsilon}{1-\epsilon}$.

Problem 3

Suppose the message space of a symmetric key encryption system is infinite (countable) with a probability distribiution on it such that $\{m \in M : \Pr(m) \neq 0\}$ is infinite. For a real number $\epsilon \in [0,1)$ we say that $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is ϵ-secure if and only if for every $m \in M$ with $\Pr(m) \neq 0$ and every $c \in C$ we have $|\frac{\Pr(m)-\Pr(m|c)}{\Pr(m)}| \leq \epsilon$.
Suppose the key space and the cipher text space are countable with a probability distribution on them. For which ϵ's there exists an ϵ-secure system on M?
(Note that the encryption is not necessarily deterministic.)

Problem 4

a) Suppose $g : \{0,1\}^n \to \{0,1\}^{n+1}$ is a PRG. Show that an attacker with an unlimited computational power can distinguish between the U_{n+1} and $g(U_n)$ with a non-negligible advantage.

b) Suppose that g is a PRG. Examine if the following functions are PRG.

b.1) $g'(x) = s||\bar{s}$

b.2) $g'(x) = s||0^{|s|}$

b.3) $g'(x) = g(s)||g(g(s))$

b.4) $g'(x) = g(0||s)||g(1||s)$

c) Suppose that X_n, Y_n, Z_n are three family of probability distributions over $\{0,1\}^n$. First define that what does it mean to say that X_n and Y_n are computationally indistinguishable, then show that if (X_n, Y_n) and (Y_n, Z_n) are computationally indistingushable then (X_n, Z_n) are also computationally indistinguishable.

d) Suppose that g is a PRG. Show that the followings are PRG.

d.1) $g'(x) = g(g(s))$

d.2) $g'(xy) = g(x)g(y); \quad \text{with } |x| = |y|.$