دانشکده‌ی علوم ریاضی

رمز نگاری — تحویل اصلی ۲۴ اسفند ۱۳۹۹

تمرین : سری ۱

مدرّس : دکتر شهرام خزائی — *تحویل نهایی ۲۹ اسفند*

- 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 1 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 15 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 `arashashoori199821@gmail.com`.

Problem 1

a) Suppose that a symmetric key encryption system has a message space M and a cipher space C. We say this system has Shannon security if for all $m_0, m_1 \in M$ and $c \in C$ we have: $\Pr(\mathsf{Enc}(k, m_0) = c) = \Pr(\mathsf{Enc}(k, m_1) = c)$; the probability is taken over a random k generated by the key generation algorithm and the randomness used by the encryption algorithm. Does Shannon security imply perfect security? What about the converse? If not, what extra condition should we put on M so that the converse holds too?
b) There are 3 people in a room. Provide a method for sharing a message with them such that any two of them together can reach the message but no one alone can reach that.

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 $\frac{|M|}{|k|} - 1$.
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 be countable with a probability distribution on it. For which ϵ's there exists an ϵ-secure system on M?