


دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری — مهلت اصلی: ۱۰ فروردین ۱۳۹۸

تمرین شماره ۲

مدرّس: دکتر شهرام خزائی — مهلت نهایی: ۱۷ فروردین ۱۳۹۸

- 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.
- 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 before hard deadline.
- You can not submit any time after hard deadline.
- All problem sets include at least 150 points which is the full score.
- Answering questions marked with (*) is mandatory.
- You can gain up to 180 points by answering unmarked questions.
- For any question contact `mr.comp97@gmail.com`

* Problem 1

Data compression is often used in data storage and transmission. Suppose you want to use data compression in conjunction with encryption. Which of the following makes more sense to do? Justify your answer. (10 Points)

1. The order does not matter – neither one will compress the data.
2. Compress then encrypt.
3. Encrypt then compress.
4. The order does not matter – either one is fine.

* Problem 2

Suppose you are told that the one time pad encryption of the message "`attack at dawn`" is "`09e1c5f70a65ac519458e7e53f36`" (the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in hex[1].). What would be the one time pad encryption of the message "`attack at dusk`" under the same OTP key? (10 Points)

* Problem 3

In this exercise, we study conditions under which the shift, mono-alphabetic substitution, and Vigenere ciphers are perfectly secret:

1. Prove that if only a single character is encrypted, then the shift cipher is perfectly secret. (5 Points)
2. Describe the largest plaintext space $\mathcal{M}$ for which the mono-alphabetic substitution cipher provides perfect secrecy (Note: this space does not need to contain words that "make sense".). (10 Points)
3. Show how to use the Vigenere cipher to encrypt any word of length n so that perfect secrecy is obtained (Note: you can choose the length of the key). Prove your answer. (10 Points)

Reconcile the above with the attacks you have learnt.

[1]See `http://en.wikipedia.org/wiki/Hexadecimal`

* Problem 4

Show that encryption scheme Π is perfectly-secret if and only if it is perfectly indistinguishable subject to experiment $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$. (20 Points)

* Problem 5

1. Suggest a formal security definition for a public key encryption system based on the following security description: (10 Points)

   > *The adversary who knows public key and ciphertext corresponding to a random message can not guess the plaintext better than a totally random guess.*

2. Show that Elgamal cryptosystem is secure with respect to the above definition under the DDH assumption. (5 Points)

Problem 6

Prove or refute: For every encryption scheme that is perfectly-secret it holds that for every distribution over the message space $\mathcal{M}$, every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$: (15 Points)

$$\Pr[M = m_1 \mid C = c] = \Pr[M = m_2 \mid C = c]$$

Problem 7

Consider the following definition of perfect secrecy for the encryption of two messages. An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ is perfectly-secret for two messages if for all distributions over $\mathcal{M}$, and for all $m_1, m_2 \in \mathcal{M}$ and $c_1, c_2 \in \mathcal{C}$ with $Pr[C_1 = c_1 \wedge C_2 = c_1] > 0$:

$$\Pr[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = \Pr[M_1 = m_1 \wedge M_2 = m_2],$$

where m_1 and m_2 are sampled independently from the same distribution over $\mathcal{M}$. Prove that no encryption scheme satisfies this definition. (15 Points)

Problem 8

Assume that we require only that an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ satisfies the following: for all $m \in \mathcal{M}$, the probability that $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$ is at least 2^{-t}. (This probability is taken over choice of k as well as any randomness

that may be used during encryption or decryption.) Show that perfect secrecy can be achieved with $\mathcal{K} < \mathcal{M}$ when $t \geq 1$. Can you prove a lower bound on the required size of $\mathcal{M}$? (15 Points)

Problem 9

As you know for a perfectly-secret encryption scheme, we have $\mathcal{K} \geq \mathcal{M}$. Prove an analogue of this theorem for the case of "almost perfect" secrecy. That is, let $\epsilon < 1$ be a constant and say we only require that for any distribution over $\mathcal{M}$, any $m \in \mathcal{M}$, and any $c \in \mathcal{C}$:

$$| \Pr[M = m \mid C = c] - \Pr[M = m] | < \epsilon$$

Prove a lower bound on the size of the key space $\mathcal{K}$ relative to $\mathcal{M}$ for any encryption scheme that meets this definition. (15 Points)

> **Hint:** Consider the uniform distribution over $\mathcal{M}$ and fix a ciphertext c. Then show that for a $(1 - \epsilon)$ fraction of the messages $m \in \mathcal{M}$, there must exist a key mapping m to c.

Problem 10

Consider a cryptosystem over message space $\mathcal{M} = \{0, 1\}$ where:

- Gen: outputs a key $k = k_0||k_1$ in $\mathcal{K} = \{00, 01, 10, 11\}$ where

$$\Pr\{K = 00\} = \Pr\{K = 11\} = 1/3$$

$$\Pr\{K = 01\} = \Pr\{K = 10\} = 1/6$$

- Enc: on input message m and key $k = k_0||k_1$ outputs $c = (m \oplus k_0)||(m \oplus k_1)$.

1. Give a precise description of the decryption algorithm (take care of $\perp$). (5 Points)
2. Is this cryptosystem perfectly secure? (15 Points)

Problem 11

Prove that $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is not (t, ϵ)-secure if Π can encrypt arbitrary length messages and the adversary is not restricted to output equal length messages in experiment $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$. (15 Points)

Problem 12

Say $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is such that for $k \in \{0,1\}^n$, algorithm Enc_k is only defined for messages of length at most $l(n)$ (for some polynomial l). Construct a scheme which is (t, ϵ)-secure even when the adversary is not restricted to output equal-length messages in experiment $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$. (15 points)

Problem 13

Show that if G is not a pseudorandom generator then the stream cipher scheme $\Pi_G = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ defined based on G - in lecture06 - does not have indistinguishable encryptions in the presence of an eavesdropper. (10 Points)

Problem 14

Show that for obtaining perfect secrecy in a symmetric encryption system, the message space must be finite. (10 points)

Problem 15

Suppose that $\mathcal{M}$ is a finite message space and Π is a public key encryption system over $\mathcal{M}$. Prove that following CPA security definitions are equivalent: (15 Points)

1. Definition1: $\forall m_0, m_1 \in \mathcal{M} : < pk, Enc_{pk}(m_0) > \simeq_c < pk, Enc_{pk}(m_1) >$
2. Definition2: The experiment defined in the book.

Problem 16

In previous question, prove that if $\mathcal{M}$ is not finite, then Definition2 does not necessarily imply Definition1. (10 Points)