دانشکدهٔ علوم ریاضی

مقدمه‌ای بر رمزنگاری — مدرس: دکتر شهرام خزایی

تمرین سری یک

گردآورنده: مهشید دهقانی، محمدحسین کلانتری — مهلت ارسال: ۴ آبان

- پاسخ‌های خود را در قالب یک فایل PDF با نام HW1-ID ارسال نمایید که ID شمارهٔ دانشجویی شما است.
- یادآوری می‌شود که در اختیار دادن راه‌حل‌های مکتوب به سایر دانشجویان و یا منتشر کردن آن در اینترنت یا شبکه‌های اجتماعی غیرمجاز است و عواقب آن بر عهدهٔ نویسنده پاسخ است.
- مشورت در تمرین‌ها مجاز است و توصیه می‌شود اما هر دانش‌جو موظف است که تمرین را به تنهایی انجام دهد و راه‌حل نهایی ارسال‌شده **باید توسط خود دانش‌جو** نوشته شده باشد. در صورت مشاهدهٔ هر گونه تخلف، نمرهٔ تمام تمرینات شخص خاطی صفر لحاظ خواهد شد.
- تمریناتی که به صورت دست‌نویس تحویل داده می‌شوند، باید به صورت کاملاً خوانا نوشته شود و با کیفیتی مطلوب و حجم پایین، اسکن و ارسال شود.
- **به ازای هر روز تاخیر، ۵ درصد از نمره‌ی کسب شده کم می‌شود. در هر سری، اجازه‌ی حداکثر ۵ روز تاخیر دارید. در مجموع کل تمرین‌ها، اجازه‌ی حداکثر ۱۰ روز تاخیر دارید.**
- **حداقل دو سری از تمرین‌ها باید با استفاده از LaTeX نوشته شده و تحویل داده شود. در غیر اینصورت ۰.۵ نمره از نمره‌ی نهایی کسر خواهد شد.**
- **لطفا فقط سه سوال را به انتخاب خود حل کنید؛ حل سوالات بیشتر نمره‌ی اضافی ندارد.**

Problem 1

Consider the following symmetric cryptosystem:

- The key generator algorithm produces a uniformly random bit as the secret key.
- The encryption algorithm receives a key $k \in \{0,1\}$ and a message $m = m_1m_2 \in \{00, 01, 10, 11\}$ where $m_1, m_2 \in \{0,1\}$ and produces a ciphertext $c = c_1c_2$ as follows:

$$c_1 = m_1 \oplus k$$
$$c_2 = m_2 \oplus k$$

1. Describe the decryption algorithm.

2. For each of the following attackers, compute the advantage, i.e.,

$$\left|\Pr[\mathrm{SKE}^{\mathrm{ps}}_{A,\Pi} = 1] - \frac{1}{2}\right|,$$

where $\mathrm{SKE}^{\mathrm{ps}}_{A,\Pi}$ is the perfect security experiment executed between an attacker A and a challenger on cryptosystem $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$, defined below:

   (a) $k \leftarrow \mathrm{Gen}()$
   (b) $m_0, m_1 \leftarrow A()$
   (c) $b \leftarrow \{0, 1\}$
   (d) $c \leftarrow \mathrm{Enc}_k(m_b)$
   (e) $\hat{b} \leftarrow A(c)$

   $\mathrm{SKE}^{\mathrm{ps}}_{A,\Pi}$ also denotes the output of the experiment which is one if $b = \hat{b}$ and zero otherwise.

   All attackers output two random and independent messages as challenge messages in phase (2). Upon receiving the ciphertext $c = c_1c_2$, the guessed bit $\hat{b}$ for attackers are as follows:

   - A_1: always outputs 1.
   - A_2: always outputs a random bit.
   - A_3: outputs 1 if $c_1 = c_2$.
   - A_4: outputs 1 if $c_1 = c_2$ and $m_0^1 = m_2^1$ where $m_0 = m_0^1 m_0^2$, otherwise it outputs a random bit.

3. Describe an attacker whose advantage is larger than that of A_4.

Problem 2

We say that $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ with message and ciphertext spaces $\mathcal{M}$ and $\mathcal{C}$ is a statistically *ϵ-indistinguishable secure SKE* if for every $m_0, m_1 \in \mathcal{M}$ and every $T \subseteq \mathcal{C}$,

$$|\Pr[\mathrm{Enc}_K(m_0) \in T] - \Pr[\mathrm{Enc}_K(m_1) \in T]| \leq \epsilon,$$

where the probabilities are taken over $K \stackrel{R}{\leftarrow} \mathrm{Gen}()$ and the coin tosses of Enc.

1. Show that statistical 0-indistinguishability is equivalent to perfect security.

2. In analogy with adversarial indistinguishability, we say that an encryption scheme $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ satisfies *ϵ-adversarial indistinguishability* if every adversary $\mathcal{A}$ succeeds at the adversarial indistinguishability experiment on page 31 in the textbook[1], with probability at most $\frac{1+\epsilon}{2}$:

[1]Jonathan Katz, Yehuda Lindell: Introduction to Modern Cryptography, Third Edition.

(a) $\mathcal{A}$ outputs a pair of messages $(\mathrm{m}_0, m_1) \in \mathcal{M}$.

(b) A random key $K \stackrel{R}{\leftarrow} \mathrm{Gen}()$ and a bit $b \stackrel{R}{\leftarrow} \{0,1\}$ are sampled. The ciphertext $c \stackrel{R}{\leftarrow} \mathrm{Enc}_K(m_b)$ is computed and given to $\mathcal{A}$.

(c) $\mathcal{A}$ outputs a bit b' and succeeds if $b = b'$.

Show that if the encryption scheme (Gen, Enc, Dec) is statistically ϵ-indistinguishable, then it also satisfies ϵ-adversarial indistinguishability.

For the next three parts, suppose (Gen, Enc, Dec) is statistically ϵ-indistinguishable for message space $\mathcal{M}$. Below you will prove that the number of keys must be at least $(1-\epsilon) \cdot |\mathcal{M}|$, therefore statistical security does not help much to overcome the limitations of perfect secrecy.

3. Call a ciphertext c *decryptable* to $m \in \mathcal{M}$ if there is a key K such that $\mathrm{Dec}_K(c) = m$. Prove that for every pair of messages $m, m' \in \mathcal{M}$,

$$\Pr[\mathrm{Enc}_K(m) \text{ is decryptable to } m'] \geq 1 - \epsilon,$$

where the probability is taken over $K \stackrel{R}{\leftarrow} \mathrm{Gen}()$ and the coin tosses of Enc.

4. Show that for every message $m \in \mathcal{M}$,

$$\mathbb{E}[\#\{m' : \mathrm{Enc}_K(m) \text{ is decryptable to } m'\}] \geq (1-\epsilon) \cdot |\mathcal{M}|,$$

where $\mathbb{E}$ represents the expected value function and again the probability is taken over K and the coin tosses of Enc. (Hint: for each m', define a random variable $X_{m'}$ that equals 1 if $\mathrm{Enc}_K(m)$ is decryptable to m', and equals 0 otherwise.)

5. Conclude that the number of keys must be at least $(1-\epsilon) \cdot |\mathcal{M}|$.

Problem 3

In this problem, we consider definitions of perfect secrecy for the encryption of two messages (using the same key). Here we consider distributions over pairs of messages from the message space $\mathcal{M}$; we let M_1, M_2 be random variables denoting the first and second message, respectively. (We stress that these random variables are not assumed to be independent.)

We generate a (single) key k, sample a pair of messages (m_1, m_2) according to the given distribution, and then compute ciphertexts $c_1 \leftarrow \mathrm{Enc}_k(m_1)$ and $c_2 \leftarrow \mathrm{Enc}_k(m_2)$; this induces a distribution over pairs of ciphertexts and we let C_1, C_2 be the corresponding random variables.

We say that an encryption scheme (Gen, Enc, Dec) is perfectly secret for two messages if for all distributions over $\mathcal{M} \times \mathcal{M}$, all $m_1, m_2 \in \mathcal{M}$, and all ciphertexts $c_1, c_2 \in \mathcal{C}$ with $\Pr[C_1 = c_1 \wedge C_2 = c_2] > 0$:

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

Prove that no such encryption scheme can exist.

Problem 4

Consider each of the following encryption schemes and state whether the scheme is perfectly secret or not. Justify your answer by giving a detailed proof if your answer is *yes*, or a counterexample if your answer is *no*.

1. An encryption scheme whose plaintext space consists of the integers $\mathcal{M} = \{0, \ldots, 12\}$ and key generation algorithm chooses a uniform key from the key space $K = \{0, \ldots, 13\}$. Suppose $\text{Enc}_k(m) = m + k \mod 13$ and $\text{Dec}_k(c) = c - k \mod 13$.

2. An encryption scheme whose plaintext space is $\mathcal{M} = \{m \in \{0,1\}^\ell \mid \text{the last bit of } m \text{ is } 0\}$ and key generation algorithm chooses a uniform key from the key space $\{0,1\}^{\ell-1}$. Suppose $\text{Enc}_k(m) = m \oplus (k\|0)$ and $\text{Dec}_k(c) = c \oplus (k\|0)$.

3. Consider an encryption scheme in which $\mathcal{M} = \{a, b\}$, $K = \{k_1, k_2, k_3, k_4\}$, and $\mathcal{C} = \{1, 2, 3, 4, 5, 6\}$. Suppose that Gen selects the secret key k according to the following probability distribution:

$$\Pr[k = k_1] = \Pr[k = k_4] = \frac{1}{6}, \quad \Pr[k = k_2] = \Pr[k = k_3] = \frac{1}{3}$$

   and the encryption matrix is as follows:

	a	b
k_1	1	4
k_2	2	3
k_3	3	2
k_4	4	1

4. Consider a variant of the one-time pad with message space $\{0,1\}^L$ where the key space $\mathcal{K}$ is restricted to all L-bit strings with an even number of 1's.

Problem 5

Let (E, D) be a one-message secure cipher defined over $(K, \mathcal{M}, \mathcal{C})$, where $\mathcal{M} = \mathcal{C} = \{0,1\}^L$. Which of the following encryption algorithms yields a one-message secure scheme? Either give an attack or provide a security proof.

1. $E_1(k, m) := 0 \parallel E(k, m)$

2. $E_2(k, m) := E(k, m) \parallel \text{parity}(m)$

3. $E_3(k, m) := \text{reverse}(E(k, m))$

4. $E_4(k, m) := E(k, \text{reverse}(m))$