دانشکده‌ی علوم ریاضی

رمز نگاری		تحویل اصلی ۵ آبان ۱۴۰۲
	تمرین : سری ۱	
مدرّس : دکتر شهرام خزائی		تحویل نهایی ۱۲ آبان

- 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 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 Parsa Reisi via `parsareisi1024q@gmail.com`.

Problem 1

We say that $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ 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 $T \subseteq \mathcal{C}$,

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

where the probabilities are taken over $K \overset{R}{\leftarrow} \mathsf{Gen}()$ 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 $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ 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 $\frac{1+\varepsilon}{2}$:

   (a) $\mathcal{A}$ outputs a pair of messages $m_0, m_1 \in \mathcal{M}$.

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

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

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

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

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

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

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

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

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

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

where 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 $\mathsf{Enc}_K(m)$ is decryptable to m', and equals 0 otherwise.)

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

Problem 2

1. For each of the following encryption schemes, describe the decryption algorithm and state whether the scheme is perfectly secret. Justify your answer in each case.

   (a) ("Two-time pad"). The plaintext is the set of all ℓ-bit strings. The key generation algorithm outputs a uniformly random key from $\{0,1\}^{\ell/2}$. To encrypt a message $m = m_1 \ldots m_\ell$ under the key $k = k_1 \ldots k_{\ell/2}$, we output $(m_1 \oplus k_1, \cdots, m_{\ell/2} \oplus k_{\ell/2}, m_{\ell/2+1} \oplus k_1, \cdots, m_\ell \oplus k_{\ell/2})$.

   (b) An encryption scheme whose plaintext space is $\mathcal{M} = \{m \in \{0,1\}^\ell |$ the last bit of m is $0\}$ and key generation algorithm chooses a uniform key from the key space $\{0,1\}^{\ell-1}$. The encryption of a message $m \in \{0,1\}^{\ell-1}$ under the key $k \in \{0,1\}^\ell$ is $E_k(m) = m \oplus (k \parallel 0)$.

   (c) Messages are ℓ bit strings. The key is a random permutation on $\{1, \ldots, 2\ell\}$. To encrypt a message m under the key k, write down m, followed by $\overline{m}$, the bitwise complement of m. Then permute the bits of the resulting 2ℓ-bit string $m \parallel \overline{m}$ according to the permutation described by k.

   (d) Same as part (c) except we replace $\overline{m}$ with 0^ℓ (here 0^ℓ denotes the sequence of ℓ zeros). That is, we apply the permutation to the 2ℓ-bit string $m \parallel 0^\ell$.

2. Give examples (with proofs) for

   (a) A scheme such that is possible to efficiently recover 90% of the bits of the key given the ciphertext, and yet it is still perfectly secure. Do you think there is a security issue in using such a scheme in practice?

(b) Given an encryption of any message, an adversary learns *nothing* about the secret key, but the scheme is completely broken (e.g., given the ciphertext, an adversary can completely recover the plaintext).

Problem 3

Suppose G is a PRG with input length λ and output length 3λ.Which of the following are PRGs? (Prove or give a counter-example for your answers)

1. $\mathsf{G}_a(s) = \mathsf{G}(s)_{[1,2\lambda]}$. That is, run G, delete the last λ bits, and output the first 2λ.
2. $\mathsf{G}_b(r, s) = (r, \mathsf{G}(s))$. Here, r, s are λ bits, and G_b has input length 2λ and output length 4λ.
3. $\mathsf{G}_c(s) = (r, \mathsf{G}(s))$. Here, r, s are λ bits, and G is a probabilistic algorithm that chooses a fresh r for each invocation.
4. $\mathsf{G}_d(s) = (s, \mathsf{G}(s))$.
5. $\mathsf{G}_e(s) = \mathsf{G}(\mathsf{G}_0(s)), \mathsf{G}(\mathsf{G}_1(s)), \mathsf{G}(\mathsf{G}_2(s))$. Here, G_0 represents the first λ bits of the output of $\mathsf{G}(s)$, G_1 the second λ bits, and G_2 the final λ bits

Problem 4

Let G be a pseudorandom generator with expansion function ℓ. Show that $\mathsf{G}(U_n)$ has a sequence of at least $2\log_2 \ell(n)$ consecutive ones with low probability (i.e. tending to 0 as $n \to \infty$). Can this probability be negligible?