CS4830 Homework 1

Instructor: Elaine Shi

Instructions

Please typeset your answers using Latex, and submit through CMS. The submission file must be in **PDF format**. We prefer to read succinct and precise answers. If you can be precise while being succinct with your answers, please try.

Due dates:

- Questions in Part I due at 11:59pm on February 24.
- Questions in Part II due at 11:59pm on March 10.

Academic integrity reminder: We treat academic integrity very seriously. You are supposed to do this homework individually. You may refer to our lecture notes and optional textbooks for help. However, should you find the solution online or by discussion with a peer, you should explicitly cite the online resource and/or your peer's name to not risk plagiarism.

Q1 Clarity, succinctness, writing your name and Netid: [**10 pts**].

Part I

Perfect Secrecy and Computational Indistinguishability

Q2 Composition of Negligible Functions. [**10 pts**]

For any two negligible functions $\epsilon_1(n)$ and $\epsilon_2(n)$, identify in each of the following cases if $\epsilon_3(n)$ is negligible. If it is negligible you need to provide a formal proof. If not, find negligible functions $\epsilon_1(n)$ and $\epsilon_2(n)$ that will serve as a counterexample.

1. $\epsilon_3(n) = \epsilon_1(n) + \epsilon_2(n)$.
2. $\epsilon_3(n) = 2\epsilon_1(n)$.
3. $\epsilon_3(n) = n\epsilon_1(n)$.
4. $\epsilon_3(n) = \frac{\epsilon_1(n)}{(\epsilon_2(n))^2}$.

Q3 Indistinguishability. [**5 pts**]

Let $\{X_n\}_{n\in\mathbf{N}}$ and $\{Y_n\}_{n\in\mathbf{N}}$ be indistinguishable ensembles. Show that

$$\{x \leftarrow X_n : \underbrace{(x, x, \ldots, x)}_{k \text{ times}}\}_{n\in\mathbf{N}} \approx \{y \leftarrow Y_n : \underbrace{(y, y, \ldots, y)}_{k \text{ times}}\}_{n\in\mathbf{N}}$$

Q4 Converse of Prediction Lemma. [**10 pts**]

Prove the converse of the prediction lemma presented in class: Let X_n^0 and X_n^1 be two distributions over $\{0,1\}^n$. Show that if there exists a PPT machine $\mathcal{A}$ such that

$$\Pr[b \leftarrow \{0,1\}; x \leftarrow X_n^b : \mathcal{A}(x) = b] \geq \frac{1}{2} + \frac{\mu}{2}$$

then there exists another PPT machine D such that,

$$\left|\Pr[x \leftarrow X_n^0 : D(x) = 1] - \Pr[x \leftarrow X_n^1 : D(x) = 1]\right| \geq \mu$$

(Hint: The same machine $\mathcal{A}$ will serve as your distinguisher D).

Q5 Perfect Security. [**10 pts**]

Alice claims to use a perfectly secret encryption scheme to encrypt messages to Bob. However, Eve shows Alice that she can recover 90% of the bits of Alice's key even after just seeing one encrypted message from Alice.

1. Explain how this is possible by constructing a perfectly secret encryption scheme which has these properties.
2. Eve claims she can always recover 10% of the message from the encryptions. Prove that this means that the encryption scheme cannot be perfectly secret.

Q6 Basic Probability. [**10 pts**]

1. A certain bacteria is thought to be present in .5% of a species. A test for this bacteria will be positive with probability .99 if it is run on an individual that has the trait and will be positive with probability .02 if it is run on an individual that does not have the trait. What is the probability that an individual that tests positive actually has this trait? (Hint: Bayes theorem)
2. A home-insurance company estimates that the probability that a particular owner will make a claim for \$5000 is 0.1, and the probability that the house and its contents will be totally destroyed is .005. Should that tragedy happen, the company will have to pay \$150,000. The company charges \$1300 for the insurance policy. What is the expected value of this policy to the insurance company? (Hint: Compute expectation)

Q7 Conditional Probability. [**5 pts**]
Two dice are tossed

1. What is the probability that you get (a) two fives (b) exactly one five (c) no fives?
2. What is the probability that the sum is 7, give that the first die is 3?
3. What is the probability that the first die is 3, given that the sum is 7?

Four cards are drawn from a standard deck

1. What is the probability that they are all hearts?
2. What is the probability that the fourth card is a heart, given that the first three cards are hearts?

Part II
PRG, PRF, and Secret Key Encryption

Q8 Pseudorandom Generators. [**10 pts**]

1. Let $g : \{0,1\}^n \to \{0,1\}^{n+1}$ be a PRG. Define the function h as follows:

$$h(z) = g(x)||g(y) \text{ where } z = x||y \text{ and } |x| = |y|$$

Prove that h is a PRG.

2. Let $f : \{0,1\}^n \to \{0,1\}^{n+1}$ and $g : \{0,1\}^n \to \{0,1\}^{n+1}$ be two pseudo-random generators (PRG), Prove or disprove the following:
   (a) The function h defined as $h(x) = g(f(x))$ is a PRG.
   (b) The function h defined as $h(x) = REVERSE(f(x))$ is a PRG, where $REVERSE(y)$ stands for the reverse of the string y.
   (c) The function h defined as $h(x) = f(x) \oplus g(x)$ is a PRG ($\oplus$ is bitwise xor).

Q9 Perfect Public Key Encryption. [**10 pts**]

Argue that a *public-key encryption* scheme cannot be *perfectly secret.* As defined before, a public-key encryption scheme $(\mathcal{M}, \mathcal{K}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is *perfectly-secret* if for all messages m_1 and m_2 in $\mathcal{M}$, and all c, k,

$$\Pr[(pk, sk) \leftarrow \mathsf{Gen}; \mathsf{Enc}_{pk}(m_1) = c \wedge pk = k] = \Pr[(pk, sk) \leftarrow \mathsf{Gen}; \mathsf{Enc}_{pk}(m_2) = c \wedge pk = k].$$

Q10 Multi-message Secure Public-Key Encryption. [**10 pts**]

In class we gave a definition for single-message secure *public-key encryption* systems. Provide a definition for many-message security and prove that it is equivalent to single-message security. Why doesn't the same proof hold in *private-key encryption* systems?

Q11 Hybrid Encryption. [**10 pts**]

Public-key encryption is typically slower than symmetric-key encryption. Therefore, when we have a long message to encrypt, it is a good idea to use the public key encryption to encrypt a symmetric key, and then use the symmetric key to encrypt the message.

Formally, let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ denote a (single-message) secure public-key encryption, and let $(\mathsf{gen}, \mathsf{enc}, \mathsf{dec})$ denote a (single-message) secure symmetric-key encryption. Consider the following public-key encryption scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$:

- $\mathsf{Gen}'(1^n)$: call $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^n)$, and output the public key pk and secret key sk.
- $\mathsf{Enc}'(\mathsf{pk}, m)$: call $k \leftarrow \mathsf{gen}(1^n)$, and output the following ciphertext:

$$\mathsf{Enc}_{\mathsf{pk}}(k), \quad \mathsf{enc}_k(m)$$

- $\mathsf{Dec}'(\mathsf{sk}, \mathsf{ct})$: parse $\mathsf{ct} := (c_0, c_1)$. Call $k := \mathsf{Dec}_{\mathsf{sk}}(c_0)$, and then call $m := \mathsf{dec}_k(c_1)$.

Please prove that this is a secure encryption scheme.