CS 435: Introduction to Cryptography **Fall 2020**

Homework 2

Professor Somesh Jha **Due:** Oct 8

1. Prove the second direction of Lemma 2.4 in the textbook. That is, show that if an encryption scheme is perfectly secret, then the condition of the equation (2.1) holds.

2. (a) Assume there is a ciphertext $\hat{c}$ such that there exists two messages m_0 and m_1 such that
$$\Pr[\mathsf{Enc}_K(m_0) = \hat{c}] > \Pr[\mathsf{Enc}_K(m_1) = \hat{c}]$$
Consider the following adversary $\mathcal{A}$ in the indistinguishability game:
if $c = \hat{c}$ **then**
guess m_0 (outputs $b' = 0$)
else
guess randomly (outputs a random bit $b' \in \{0, 1\}$)
end if
What is the probability of $\mathcal{A}$ winning the game?
   (b) Now argue that definition III (indistinguishability game) implies definition II (equation (2.1) in the textbook).

3. Consider the encryption scheme of Homework 1 (question 4(b)).
   (a) Let $n = 5$. Given the ciphertext $c = 1000111001$, consider the following message space:
$$\mathcal{M}(c) = \{m \mid m = \mathsf{Dec}_k(c) \text{ for some } k \in \mathcal{K}\}$$
(we used this in the bad news theorem). Show a message m such that $m \notin \mathcal{M}(c)$.
   (b) Now take arbitrary n and $c \in \{0, 1\}^{2n}$. Show how to get m which is not in $\mathcal{M}(c)$.

4. Let $f(n)$ be a negligible function and k a positive integer. Prove the following:
   (a) $f(\frac{n}{k})$ is negligible.
   (b) $f(n^{1/k})$ is negligible.
   (c) $a(n)f(n)$ is negligible where $a(n)$ is polynomially bounded (i.e., there exists a positive polynomial $r(n)$ such that $r(n) > a(n)$ asymptotically).