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.

   Solution: Say $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is perfectly secret. For two messages m, m' and a ciphertext c, perfect secrecy implies that $\Pr[M = m \mid C = c] = \Pr[M = m]$ and $\Pr[M = m' \mid C = c] = \Pr[M = m']$. We can find that

$$\begin{aligned}\Pr[\mathsf{Enc}_K(m) = c] &= \Pr[\mathsf{Enc}_K(M) = c \mid M = m] = \Pr[C = c \mid M = m] \\ &= \frac{\Pr[M = m \mid C = c] \cdot \Pr[C = c]}{\Pr[M = m]} = \frac{\Pr[M = m] \cdot \Pr[C = c]}{\Pr[M = m]}\end{aligned}$$

   An analogous calculation holds for m' as well, and we obtain $\Pr[\mathsf{Enc}_K(m') = c] = \Pr[C = c]$. Therefore, we conclude that $\Pr[\mathsf{Enc}_K(m) = c] = \Pr[\mathsf{Enc}_K(m') = c]$. ■

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).

   Solution:

   (a) We have

$$\Pr[\mathsf{PrivK}^{\mathsf{env}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{env}}_{\mathcal{A},\Pi} = 1 \mid M = m_0] + \frac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{env}}_{\mathcal{A},\Pi} = 1 \mid M = m_1] \tag{1}$$

   since each message is chosen with probability 1/2 in indistinguishability game. Then,

$$\begin{aligned}\Pr[\mathsf{PrivK}^{\mathsf{env}}_{\mathcal{A},\Pi} = 1 | M = m_0] &= \Pr[\mathsf{Enc}_K(m_0) = \hat{c}] + \frac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_0) \neq \hat{c}] \\ &= \Pr[C = \hat{c} \mid M = m_0] + \frac{1}{2} \cdot \Pr[C \neq \hat{c} \mid M = m_0]\end{aligned} \tag{2}$$

where the first term is because $\mathcal{A}$ always outputs 0 when receiving $\hat{c}$ (and when $M = m_0$ this means that $\mathsf{PrivK}^{\mathsf{env}}_{\mathcal{A},\Pi} = 1$), and the second term is because $\mathcal{A}$ outputs a random bit when given a ciphertext $c \neq \hat{c}$. A similar analysis for the case that $M = m_1$ gives

$$\begin{aligned}
\Pr[\mathsf{PrivK}^{\mathsf{env}}_{\mathcal{A},\Pi} = 1|M = m_1] &= 0 \cdot \Pr[\mathsf{Enc}_K(m_1) = \hat{c}] + \frac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_1) \neq \hat{c}] \\
&= \frac{1}{2} \cdot \Pr[C \neq \hat{c} \mid M = m_1] \qquad (3)
\end{aligned}$$

By inserting (2) and (3) to (1), we have

$$\begin{aligned}
\Pr[\mathsf{PrivK}^{\mathsf{env}}_{\mathcal{A},\Pi} = 1] &= \frac{1}{2} \cdot (\Pr[C = \hat{c} \mid M = m_0] + \frac{1}{2} \cdot \Pr[C \neq \hat{c} \mid M = m_0]) \\
&\quad + \frac{1}{2} \cdot \frac{1}{2} \cdot \Pr[C \neq \hat{c} \mid M = m_1] \\
&= \frac{1}{2} \cdot (\Pr[C = \hat{c} \mid M = m_0] + \frac{1}{2} \cdot (1 - \Pr[C = \hat{c} \mid M = m_0])) \\
&\quad + \frac{1}{2} \cdot \frac{1}{2} \cdot \Pr[C \neq \hat{c} \mid M = m_1 \\
&= \frac{1}{4} + \frac{1}{4} \Pr[C = \hat{c} \mid M = m_0] + \frac{1}{4} \Pr[C \neq \hat{c} \mid M = m_1] \\
&> \frac{1}{4} + \frac{1}{4} \Pr[C = \hat{c} \mid M = m_1] + \frac{1}{4} \Pr[C \neq \hat{c} \mid M = m_1] \\
&= \frac{1}{4} + \frac{1}{4} = \frac{1}{2}
\end{aligned}$$

where the inequality is by the given assumption of the problem description. Since the probability of $\mathcal{A}$ winning the game $\Pr[\mathsf{PrivK}^{\mathsf{env}}_{\mathcal{A},\Pi} = 1]$ is greater than 1/2, it is not perfectly indistinguishable.

(b) In (a), we have shown that non-perfect secrecy implies distinguishability. This becomes contrapositive of the statement that indistinguishability (definition III) implies perfect secrecy with respect to definition II. Hence, we can argue that any perfectly indistinguishable encryption scheme is also perfectly secret.

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 $\mathcal{M}(c)$.

Solution:

(a) Since $n = 5$, the first and sixth bits of m are encrypted to 1 both by the first bit of k (say k_1). Hence, no plaintext whose first and sixth bits are different can be encrypted to the given c because k_1 that satisfies $1 \oplus k_1 = 1$ and $0 \oplus k_1 = 1$ does not exist. For instance, $m = 1000101001$ is not in $\mathcal{M}(c)$.

(b) Let m_i, c_i and k_i be the ith bit of plaintext m, ciphertext c and key k, respectively. We know that $m_i \oplus k_i = c_i$ and $m_{i+n} \oplus k_i = c_{i+n}$ for $\forall i \in [n]$. Given arbitrary c and n, we can come up with m such that $m \notin \mathcal{M}(c)$ based on the following rules: for $i = 1, 2, ..., n$

   i. if $c_i = c_{i+n}$, then set $m_i \neq m_{i+n}$. This results in $m_i \oplus k_i \neq m_{i+n} \oplus k_i$, which means that no k_i can make m_i and m_{i+n} to be encrypted to the same bit.

   ii. if $c_i \neq c_{i+n}$, then set $m_i = m_{i+n}$. This results in $m_i \oplus k_i = m_{i+n} \oplus k_i$, which means that no k_i can make m_i and m_{i+n} to be encrypted to different bits.

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).

Solution:

(a) Let $p(n)$ be a positive polynomial. As k is positive, the function $q(n) = p(kn)$ is also a positive polynomial and because $f(n)$ is negligible, for some N we have

$$f(n) < \frac{1}{q(n)} = \frac{1}{p(kn)}, \quad \forall n > N.$$

Substituting $n \mapsto \frac{n}{k}$ it follows that

$$f(\frac{n}{k}) < \frac{1}{p(n)}, \quad \forall n > kN.$$

Since $p(n)$ was arbitrarily chosen, we conclude that $f(\frac{n}{k})$ is also negligible.

(b) Let $p(n)$ be a positive polynomial. As k is a positive integer, the function $q(n) = p(n^k)$ is also a positive polynomial and because $f(n)$ is negligible, for some N we have

$$f(n) < \frac{1}{q(n)} = \frac{1}{p(n^k)}, \quad \forall n > N.$$

Substituting $n \mapsto n^{1/k}$ it follows that

$$f(n^{1/k}) < \frac{1}{p(n)}, \quad \forall n > N^k.$$

Since $p(n)$ was arbitrarily chosen, we conclude that $f(n^{1/k})$ is also negligible.

(c) Since $a(n)$ is polynomially bounded, $a(n)f(n) < r(n)f(n)$, for $\forall n > N_1$. Let $p(n)$ be a positive polynomial. Since $r(n)p(n)$ is still a positive polynomial and $f(n)$ is negligible, $f(n) < \frac{1}{r(n)p(n)}$, for $\forall n > N_2$. Putting these together, we have

$$a(n)f(n) < r(n)f(n) < \frac{1}{p(n)}, \quad \forall n > max\{N_1, N_2\}$$

Since $p(n)$ was arbitrarily chosen, we conclude that $a(n)f(n)$ is also negligible.