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

Homework 2

Professor Somesh Jha **Due:** Feb 26 (Midnight)

1. Exercise 2.4 from the textbook.

   Solution: Assume the scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ is perfectly secret. That is, for all $m \in \mathcal{M}$ and $c \in \mathcal{C}$ such that $\Pr[C = c] > 0$,

   $$\Pr[M = m \mid C = c] = \Pr[M = m]$$

   If $c \in \mathcal{C}$ has $\Pr[C = c] = 0$, then clearly $\Pr[\mathsf{Enc}_k(m) = c] = 0 = \Pr[\mathsf{Enc}_k(m') = c]$ for any pair of messages $m, m' \in \mathcal{M}$. With this in mind, let m, m' be arbitrary messages in $\mathcal{M}$ and $c \in \mathcal{C}$ with $\Pr[C = c] > 0$, then

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

   and similarly we have $\Pr[\mathsf{Enc}_k(m') = c] = \Pr[C = c \mid M = m']$. Now, using Bayes' Theorem, we get

   $$\Pr[C = c \mid M = m] = \frac{\Pr[M = m \mid C = c]\Pr[C = c]}{\Pr[M = m]}.$$

   Then, by perfect secrecy,

   $$\begin{aligned}\Pr[C = c \mid M = m] &= \frac{\Pr[M = m]\Pr[C = c]}{\Pr[M = m]} \\ &= \Pr[C = c].\end{aligned}$$

   Again, the same can be shown for m'. Therefore, $\Pr[\mathsf{Enc}_k(m) = c] = \Pr[C = c] = \Pr[\mathsf{Enc}_k(m') = c]$, concluding the proof.

2. Prove Theorem 2.9 using definition II (equation (2.1) in the textbook).

   Solution: Using similar reasoning as in the proof of Theorem 2.9, for any $m \in \mathcal{M}$ we get

   $$\Pr[\mathsf{Enc}_K(m) = c] = \Pr[m \oplus K = c] = \Pr[K = m \oplus c] = 2^{-l},$$

   Since $m \in \mathcal{M}$ is a generic message, we also have $\Pr[\mathsf{Enc}_K(m') = c] = 2^{-l} = \Pr[\mathsf{Enc}_K(m) = c]$ for any $m, m' \in \mathcal{M}$ and we are done.

3. Consider a scheme $\text{OTP}' = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ where $\mathcal{K} = \{0,1\}^\ell$, $\mathcal{M} = \{0,1\}^{2\ell}$ and $\mathcal{C} = \{0,1\}^{2\ell}$. Gen generates a random ℓ-bit string as a key, $\mathsf{Enc}_k(m) = kk^R \oplus m$ (where k^R is the reverse of ℓ-bit string k) and $\mathsf{Dec}_k(c) = kk^R \oplus c$.

Does the scheme work? Prove using definition III (indistinguishability game) that this scheme is not perfectly secret.

Solution: We model this solution after the proof in the book that the Vigenère cipher is not perfectly secret using the indistinguishability game (check Example 2.7 on pages 31 and 32). We define adversary $\mathcal{A}$ to do the following:

(a) Output $m_0 = 0^{2\ell}$ and $m_1 = 0^{2\ell-1}1$.

(b) Upon receiving challenge ciphertext $c = c_1 c_2 \dots c_{2\ell}$, do the following: if $c_1 = c_{2\ell}$, then output 0, otherwise output 1.

Now we compute the probability that $\mathcal{A}$ succeeds,

$$\begin{aligned}\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi} = 1] &= \frac{1}{2}\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 0] + \frac{1}{2}\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 1] \\ &= \frac{1}{2}\Pr[\mathcal{A} \text{ outputs } 0 \mid b = 0] + \frac{1}{2}\Pr[\mathcal{A} \text{ outputs } 1 \mid b = 1].\end{aligned}$$

Note that if $b = 0$, then $c = kk^R$, the key k followed by its reverse, and then it is guaranteed that $c_1 = c_{2\ell}$ independent of which key k is chosen to produce c. In this case, we get that $\Pr[\mathcal{A} \text{ outputs } 0 \mid b = 0] = 1$. On the other hand, if $b = 1$, then $c_1 = 0 \oplus k_1 = k_1$, the first bit of key k, and $c_{2\ell} = 1 \oplus k_1 = \overline{k_1}$, the negation of the first bit of k. Thus, it is impossible for c_1 to equal $c_{2\ell}$, and again we get $\Pr[\mathcal{A} \text{ outputs } 1 \mid b = 1] = 1$. Plugging back into the previous equation we get $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi} = 1] = 1$, that is, adversary $\mathcal{A}$ actually succeeds in the game with probability 1. Since this is larger than 1/2, we conclude that the given cipher is not perfectly secret.

4. Let $f(n)$ be a negligible function and k a positive integer. Prove the following:

(a) $f(\sqrt{n})$ is negligible.

(b) $f(\frac{n}{k})$ is negligible.

(c) $f(n^{1/k})$ is negligible.

Solution:

(a) Let $p(n)$ be a positive polynomial. Then the function $q(n) = p(n^2)$ is also a positive polynomial and because $f(n)$ is negligible, for some N we have

$$f(n) < \frac{1}{q(n)} = \frac{1}{p(n^2)}, \quad \forall n > N.$$

Substituting $n \mapsto \sqrt{n}$ it follows that

$$f(\sqrt{n}) < \frac{1}{p(n)}, \quad \forall n > N^2.$$

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

(b) 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

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

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

(c) 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.