Homework 3

1. **Equivalent definition of Perfect Secrecy.** In the lecture we defined the perfect security for any private-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as follows. For any message m, cipher-text c, and a priori probability distribution $\mathbb{M}$ over the set of messages, we have:

$$\mathbb{P}\left[\mathbb{M} = m \middle| \mathbb{C} = c\right] = \mathbb{P}\left[\mathbb{M} = m\right]$$

(40 points) Show that the above definition is equivalent to the following alternative definition. For all messages m, m', cipher-text c, and a priori probability distribution $\mathbb{M}$ over the set of messages, we have:

$$\mathbb{P}\left[\mathbb{C} = c \middle| \mathbb{M} = m\right] = \mathbb{P}\left[\mathbb{C} = c \middle| \mathbb{M} = m'\right],$$

Remarks: (1) Proving equivalence means that you have to show that the first definition implies the second definition. And, the second definition also implies the first definition.

(2) Additionally, in this problem, for simplicity, assume that in the the probability expressions no "division by error" occurs.

Solution.

2. **Defining Perfect Security from Ciphertexts.** An upstart in the field of cryptography has proposed a new definition for perfect security of private-key encryption schemes. According to this new definition, a private-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is perfectly secure, if, for all a priori distribution $\mathbb{M}$ over the message space, and any two cipher-texts c and c', we have the following identity.

$$\mathbb{P}\left[\mathbb{C} = c\right] = \mathbb{P}\left[\mathbb{C} = c'\right]$$

(20 points) Show that the definition in the class does not imply this new definition.

Remark. You need to construct a private-key encryption scheme that is secure according to the definition we learned in the class. However, this scheme does not satisfy the new definition.

Solution.

3. **One-time Pad for 3-Alphabet Words.** We interpret $a, b, \dots, z$ as $0, 1, \dots, 25$. We will work over the group $(\mathbb{Z}_{26}^3, +)$, where $+$ is coordinate-wise integer-sum $\mod 26$. For example, $abx + acd = ada$.

   Now, consider the one-time pad encryption scheme over the group $(\mathbb{Z}_{26}^3, +)$.

   (a) (5 points) What is the probability that the encryption of the message *cat* is the cipher text *cat*?
   Solution.

(b) (5 points) What is the probability that the encryption of the message *cat* is the cipher text *dog*?
Solution.

4. **A Conjectured Private-key Encryption Scheme.** Consider the following encryption scheme.

- The message space $\mathcal{M}$ is the set of all n-bit strings that have exactly t-ones in them.
- The key space $\mathcal{K}$ is the set of all permutations from the set $\{1, 2, \dots, n\}$ to $\{1, 2, \dots, n\}$.
- The set of all cipher-texts, represented by $\mathcal{C}$, is identical to $\mathcal{M}$.

The private-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is defined below.

- $\mathsf{Gen}()$: Return a random permutation sk from $\{1, 2, \dots, n\}$ to $\{1, 2, \dots, n\}$.
- $\mathsf{Enc}_{\mathsf{sk}}(m)$: Return c, where c is obtained by permuting the message m using the permutation sk. For example, if $m = m_1 m_2 \dots m_n$, then the permutation of m using sk is the string $c = c_1 c_2 \dots c_n = m_{\mathsf{sk}(1)} m_{\mathsf{sk}(2)} \dots m_{\mathsf{sk}(n)}$.
- $\mathsf{Dec}_{\mathsf{sk}}(c)$: Return $\widetilde{m}$, where $\widetilde{m}$ is obtained from c by inverting the permutation sk. For example, if $c = c_1 c_2 \dots c_n$, then decoded message is $c_{\mathsf{sk}^{-1}(1)} c_{\mathsf{sk}^{-1}(2)} \dots c_{\mathsf{sk}^{-1}(n)}$.

(30 points) Is this scheme perfectly secure? If yes, then provide a proof. If no, then give a counterexample.

A worked-out example of the encryption algorithm. Let $n = 4$ and $t = 2$. Therefore, we have the set of messages $\mathcal{M} = \{1100, 1010, 1001, 0110, 0101, 0011\}$. Note that the size of the set $\mathcal{M}$ is $\binom{n}{t} = 6$. The set $\mathcal{K}$ is the set of all permutations from the set $\{1, 2, 3, 4\}$ to the set $\{1, 2, 3, 4\}$. Note that there are a total of $4! = 24$ such permutations.

Suppose the $\mathsf{Gen}()$ algorithm picked the following permutation

$$\mathsf{sk}(1) = 3, \mathsf{sk}(2) = 1, \mathsf{sk}(3) = 4, \mathsf{sk}(4) = 2$$

Suppose Alice wants to encrypt the message $m = m_1 m_2 m_3 m_4 = 1010$ using the sk above. Then, the cipher-text is $c = m_{\mathsf{sk}(1)} m_{\mathsf{sk}(2)} m_{\mathsf{sk}(3)} m_{\mathsf{sk}(4)} = m_3 m_1 m_4 m_2 = 1100$. When Bob wants to decrypt the message $c = c_1 c_2 c_3 c_4 = 1100$, he outputs $\widetilde{m} = c_{\mathsf{sk}^{-1}(1)} c_{\mathsf{sk}^{-1}(2)} c_{\mathsf{sk}^{-1}(3)} \widetilde{c}_{\mathsf{sk}^{-1}(4)} = c_2 c_4 c_1 c_3 = 1010$.

Note that in the example presented above, we recovered the original message! However, is this scheme secure?

Solution.

Collaborators :