Cryptography Exercise Sheet 5

Prof. Dr. Thomas Wilke, Dr.-Ing. Kim-Manuel Klein

29. April 2020

1. **Problem:** *Double encryption (Exercise 5.1 in BS)*

   Let $\mathcal{E} = (E, D)$ be a cipher. Consider the cipher $\mathcal{E}_2 = (E_2, D_2)$, where $E_2(k, m) = E(k, E(k, m))$. One would expect that if encrypting a message once with E is secure then encrypting it twice as in E_2 should be no less secure. However, that is not always true.

   (a) Show that there is a semantically secure cipher $\mathcal{E}$ such that $\mathcal{E}_2$ is not semantically secure.

   (b) Prove that for every CPA secure ciphers $\mathcal{E}$, the cipher $\mathcal{E}_2$ is also CPA secure. That is, show that for every CPA adversary $\mathcal{A}$ attacking $\mathcal{E}_2$ there is a CPA adversary $\mathcal{B}$ attacking $\mathcal{E}$ with about the same advantage and running time.

2. **Problem:** *An alternate definition of CPA security (Exercise 5.3 in BS)*

   This exercise develops an alternative characterization of CPA security for a cipher $\mathcal{E} = (E, D)$, defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. As usual, we need to define an attack game between an adversary $\mathcal{A}$ and a challenger. Initially, the challenger generates

   $$b \xleftarrow{R} \{0, 1\}, k \xleftarrow{R} \mathcal{K}. \tag{1}$$

   Then $\mathcal{A}$ makes a series of queries to the challenger. There are two types of queries:

   Encryption: In an *encryption query*, $\mathcal{A}$ submits a message $m \in \mathcal{M}$ to the challenger, who responds with a ciphertext $c \xleftarrow{R} E(k, m)$. The adversary may make any (poly-bounded) number of encryption queries.

   Test: In a *test query*, $\mathcal{A}$ submits a pair of messages $m_0, m_1 \in \mathcal{M}$ to the challenger, who responds with a ciphertext $c \xleftarrow{R} E(k, m_b)$. The adversary is allowed to make only a *single* test query (with any number of encryption queries before and after the test query).

   At the end of the game, $\mathcal{A}$ outputs a bit $\hat{b} \in \{0, 1\}$.

   As usual, we define $\mathcal{A}$s advantage in the above attack game to be $|Pr[\hat{b} = b] - 1/2|$. We say that $\mathcal{E}$ is Alt-CPA secure if this advantage is negligible for all efficient adversaries.

   Show that $\mathcal{E}$ is CPA secure if and only if $\mathcal{E}$ is Alt-CPA secure.

3. **Problem:** *Ciphertext expansion vs. security (Exercise 5.10 in BS)*

   Let $\mathcal{E} = (E, D)$ be an encryption scheme where messages and ciphertexts are bit strings.

   (a) Suppose that for all keys and all messages m, the encryption of m is the exact same length as m. Show that (E, D) cannot be semantically secure under a chosen plaintext attack.

(b) Suppose that for all keys and all messages m, the encryption of m is exactly ℓ bits longer than the length of m. Show an attacker that can win the CPA security game using $\approx 2^{\ell/2}$ queries and advantage $\approx 1/2$. You may assume the message space contains many more than $2^{\ell/2}$ messages.