Second assignment

Cryptography, ITC8240

November 2021

1 Important notices:

- If you have any questions regarding the tasks, please do not hesitate to contact me.
- This assignment is Pass or Fail. To pass you need to get at least 50% of the total points for compulsory tasks (13 out of 26).
- **Provide an explicit explanation to your solutions**. Providing answers to the task with no explanation will give you 0 points.
- Your solution should be in the PDF format. You may either scan a handwritten solution or type your solution (Word, TXT, LaTeX, etc.) and export it into PDF.
- For submitting your solution in a LaTeX, you get up 2 bonus points.
- If you get more than 100% of the total points (by solving bonus tasks), that will positively affect your final mark.
- You may write the programming code to solve any task. However, you have to explain explicitly the code logic in your submission and how it helped you solving the task. Providing the code with no explanations will give you 0 points for the task. You must submit your code either in the appendix of your submission or to a public repository (GitHub, Bitbucket, Gitlab).
- **Bruteforce is not a solution!**

- Using online tools or/and someone's else code to solve the tasks is prohibited. If you are suspected of this, then you will receive 0 for the task.
- Plagiarism is prohibited. If you are suspected of this, then you will receive 0 for the task and will be reported to the Dean's office.
- This assignment is due 24th of November, 2 pm. If you submit later the due date, that will negatively affect your final mark.

2 Assignment tasks

2.1 Task 1 (6 points) - Key establishment

As an experienced cryptographer, you are approached with the following question. There are three friends (secret agents) Alex, Bob and Connie. They want to generate a common secret key so they can exchange secret messages. Your task is to design an extension of the Diffie-Hellman protocol that helps them to generate the key. Please, provide detailed explanation of your solution.

2.2 Task 2 (6 points) - Block ciphers

Alice wants to send message m, encrypted with block cipher, to Bob. The message m is split into 6 blocks of equal length $m = m_0||m_1||m_2||m_3||m_4||m_5$ and encrypted using DES. However, a transmission error occurs (or malicious Carol got access to the channel) and one bit of the ciphertext c_2 changes its value.

Bob receives the ciphertexts, decrypts them and gets the following message $m' = m'_0||m'_1||m'_2||m'_3||m'_4||m'_5$. Please, explain to Bob how many bits are expected to be wrong in each block m'_i if Alice used ECB mode and if Alice used CBC mode.

2.3 Task 3 (8 points) - Security definitions and proofs

Consider the following security definition:

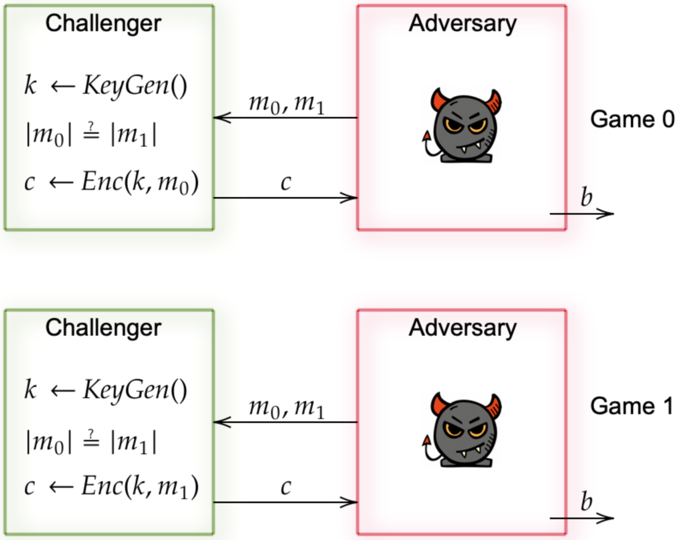


Figure 1: Security games

The encryption scheme satisfies the security definition if it holds that $|Pr[b = 1 : \text{Game } 0] - Pr[b = 1 : \text{Game } 1]| \leq \epsilon$, where ϵ is negligible. Intuitively, it means that no adversary, upon seeing encryption of m_0 or m_1, can guess which of the two messages has been encrypted. Note, that adversary is allowed to do only ONE query and the messages should have equal length.

Show that OTP (one time pad) in CBC mode does not satisfy the security definition, by describing an attack.

HINT: Start with writing out, how the ciphertext blocks are constructed in this scheme and think, how you could use properties of XOR operation.

2.4 Task 4 O-notation (6 points)

- Show that $O(n^3) = 11n^3 + 4n^2 + 9n - 36$
- Show that $O(n^4) = 5n^4 - 4n^2 - 4$

3 Bonus Tasks

3.1 Task 1 (6 points) - Block ciphers and security definitions

Suppose F is a secure PRF with input length n. We want to use F to construct a PRF with longer input length $(2n)$ and use the following approach:

$$F'(k, x||x') = F(k, x)||F(k, x'), \text{ where } x, x' \in \{0,1\}^n.$$

Your task is to describe a successful distinguishing attack that shows that new function F' **is not PRF**.

Definition – Pseudo-Random Function (PRF)
Let $F_K : \{0,1\}^n \to \{0,1\}^n$ be a function that depends on a random key $k \in \mathcal{K}$, where $\mathcal{K}$ is a key space. Let $\mathcal{F}$ be a set of all functions of the form $f : \{0,1\}^n \to \{0,1\}^n$. Now, let us define the following games:

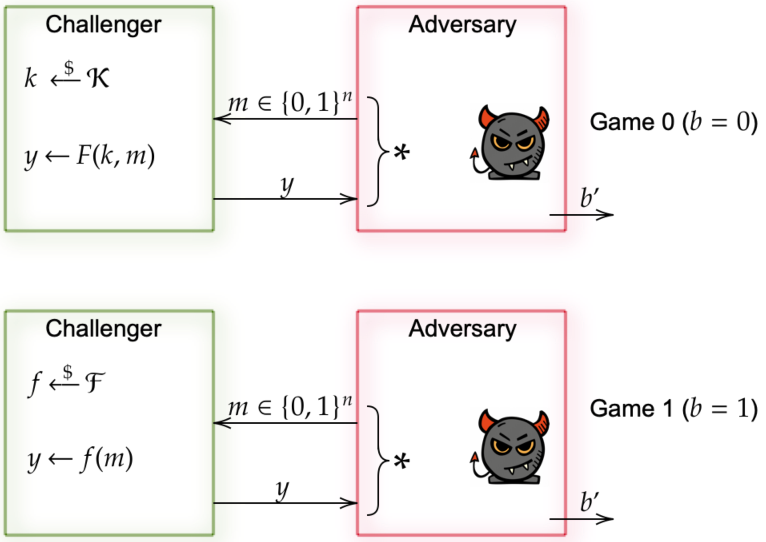


Figure 2: Security games

The adversary may submit several queries to the challenger. At the end, the adversary computes and outputs a bit $b' \in 0, 1$. The function F_K satisfies the security definition if it holds that

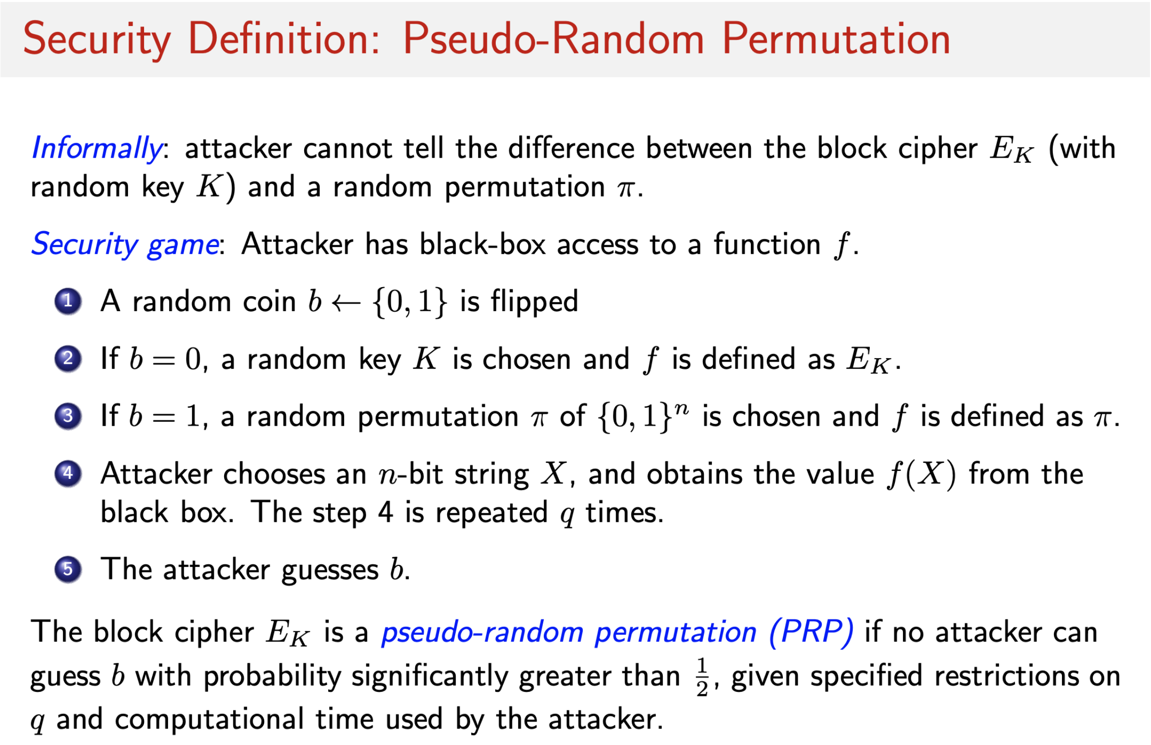
$$|Pr[b = 1 : \text{Game } 0] - Pr[b = 1 : \text{Game } 1]| \leq \epsilon,$$

where ϵ is negligible. Please, also take a look at the definition from the slides (Week 5: Block Ciphers).

HINT 1: Even in the case of a "random function" (Game 1), the function f itself is still deterministic!

3.2 Task 2 (3 points) - Security definitions

Consider the following security definition (from the lecture slides):



Security Definition: Pseudo-Random Permutation

Informally: attacker cannot tell the difference between the block cipher E_K (with random key K) and a random permutation π.

Security game: Attacker has black-box access to a function f.

1. A random coin $b \leftarrow \{0, 1\}$ is flipped
2. If $b = 0$, a random key K is chosen and f is defined as E_K.
3. If $b = 1$, a random permutation π of $\{0, 1\}^n$ is chosen and f is defined as π.
4. Attacker chooses an n-bit string X, and obtains the value $f(X)$ from the black box. The step 4 is repeated q times.
5. The attacker guesses b.

The block cipher E_K is a *pseudo-random permutation (PRP)* if no attacker can guess b with probability significantly greater than $\frac{1}{2}$, given specified restrictions on q and computational time used by the attacker.

Figure 3: Pseudo-Random Permutation

Your task is to draw security games between the challenger and adversary that correspond to the definition above. Note that Figure 1 and Figure 2 will help you to solve the task.