**Second homework**

# 1 Important notices:

- **If you have any questions regarding the tasks, please do not hesitate to contact instructors.**
- This assignment gives you 15% of the final grade.
- **Provide an explicit explanation to your solutions**. Providing answers to the task with no explanation will give you $0$ points.
- Your solution must be in the PDF format. You may either scan a handwritten solution or type your solution in Latex (LaTeX) or MS Word. Then export it into PDF. **Solutions submitted in a non-PDF format will receive $0$ points**.
- 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 or Gitlab).
- You may use any online or installed tools to solve a task. However, you must explain how exactly tool helped you solve the task and your personal contribution. The tool must be properly referenced.
- **Plagiarism is prohibited.** Any used sources of information must be referenced. If you are suspected of plagiarism, then you will receive $0$ for the task and will be reported to the Dean's office and Program Manager.
- This assignment is due **30th of March, 23:59**.

| Letter | Binary | Integer value | Letter | Binary | Integer value |
|---|---|---|---|---|---|
| A | 00000 | 0 | O | 01110 | 14 |
| B | 00001 | 1 | P | 01111 | 15 |
| C | 00010 | 2 | Q | 10000 | 16 |
| D | 00011 | 3 | R | 10001 | 17 |
| E | 00100 | 4 | S | 10010 | 18 |
| F | 00101 | 5 | T | 10011 | 19 |
| G | 00110 | 6 | U | 10100 | 20 |
| H | 00111 | 7 | V | 10101 | 21 |
| I | 01000 | 8 | W | 10110 | 22 |
| J | 01001 | 9 | X | 10111 | 23 |
| K | 01010 | 10 | Y | 11000 | 24 |
| L | 01011 | 11 | Z | 11001 | 25 |
| M | 01100 | 12 | | | |
| N | 01101 | 13 | | | |

Table 1: Conversion table (for task 4)

# Tasks

**Task 1. Confusion and diffusion** From the lectures, you learned about importance of **confusion** and **diffusion** principles for the block ciphers. Let us examine them in more details. Assume you need to analyse properties of Vigenere cipher.

1. Encrypt message THEWANDCHOOSESTHEWIZARD with key MAGIC.
2. Suppose we change one letter (**W** becomes **L**) in the plaintext to get THEWANDCHOOSESTHE **L** IZARD. How may letters of the ciphertext are changed? Is the diffusion property achieved?
3. Suppose we change one letter in key (**G** becomes **N**). How may letters of the ciphertext are changed? Is confusion property achieved?

**Task 2. Pseudorandom function** Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be **a secure PRF**. Do the following functions satisfy definition of pseudo-random function?

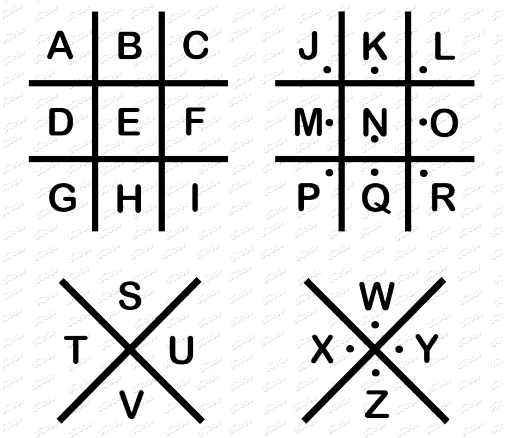
- $F'(k,m) = F(k,m)||0^n$, where $0^n$ is a zero string of length $n$.
- $F'(k,m||m') = F(k,m)||F(k,m' \oplus 0^n)$, where $0^n$ is a zero string of length $n$.
- $F'(k,m||m') = F(k,0||m) \oplus F(k,m'||1)$, where $m, m' \in \{0,1\}^{n-1}$.

**Task 3. Output feedback mode** Consider the following **permutation cipher** – instead of permuting plaintext letters to get ciphertext, you are first required to convert plaintext letters to binary form and next you permute bits according to the key. Letter H becomes encrypted to T with key $(5,1,2,4,3)$. Let us view it as block cipher with block length $5$ bits.

1. Encrypt world DOG with key $(4,1,3,5,2)$ using permutation cipher in OFB mode with $iv = 01011$. Leave result as a binary string.
2. Flip $5$-th bit of received ciphertext ($0$ becomes $1$ and vice versa). Now decrypt modified ciphertext. How many bits in the plaintext get changed?
3. Flip the first bit of the IV $iv' = 11011$, decrypt ciphertext from Step 1 with $iv'$. How many bits in the plaintext get changed?

**Task 4.** Consider the encryption of $n-$block message $m = m_1||m_2||\ldots||m_n$ by some block cipher $E$ in **CFB** mode. Let use denote ciphertext produced by $E$ as $c = c_1||c_2||\ldots||c_n$. Show which information about the plaintext can be extracted if we get a collision: $c_i = c_j$, where $i \neq j$.

**Task 5.** Show that Pigpen cipher defined below is not **IND-OT-CPA** secure (where adversary is allowed to do only one query to the challenger in the IND-CPA game).
The pigpen cipher uses graphical symbols assigned according to a key in the diagram below[1] (**NOTE**: Positions of the letters in the diagrams are random and not known to adversary):




[1] `https://en.wikipedia.org/wiki/Pigpen_cipher` and `https://www.dcode.fr/pigpen-cipher`

**Bonus Task** Consider the following security definition:

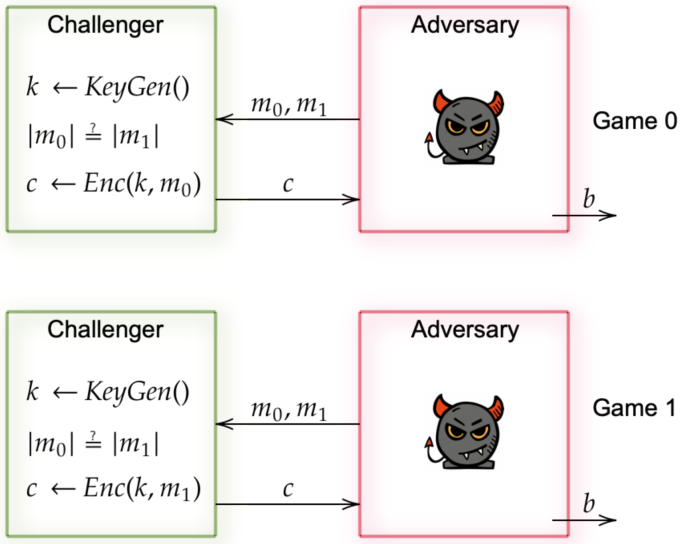



Figure 1: Security games

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 $\epsilon$ is negligible. Intuitively, it means that no adversary, upon seeing encryption of $m_0$ or $m_1$ (those are **not blocks** of the plaintext, but **two distinct messages** which could be a size of multiple blocks), 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.