First assignment

Cryptography, ITC8240

October 2021

1 Important notices:

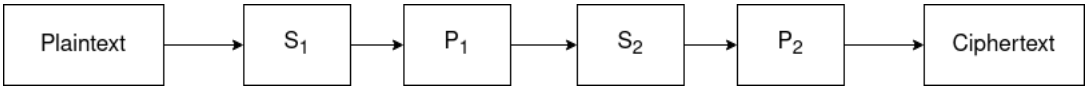
- This assignment is Pass or Fail. To pass you need to get at least 51% of the total points for compulsory tasks (14 out of 27).
- Provide an explicit explanation to your solutions. Providing answers to the task with no explanation will give you 0 points.
- Your solution should be in the PDF format. 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).
- 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 18th of October, 9 am. If you submit later the due date, that will negatively affect your final mark.

2 Assignment tasks

2.1 Task 1 (8 points)

Consider the following sequence of operations:



Plaintext is **BLOCKCHAIN**. S_1 is a shift cipher with key $k_{S_1} = 9$. S_2 is a shift cipher with the key $k_{S_2} = 19$. P_1 is a permutation cipher with a key $k_{P_1} = (5, 1, 3, 2, 4)$. P_2 is a permutation cipher with a key $k_{P_2} = (3, 1, 4, 2, 5)$. **The task:** what is the ciphertext?

2.2 Task 2 (6 points)

Consider the following plaintext:

FRIENDSMAKETHEWORSTENEMIES

1. Encrypt the plaintext using Vigenere cipher with the key k=**LIST**
2. Calculate the index of coincidence of the plaintext.
3. Calculate the index of coincidence of the ciphertext.

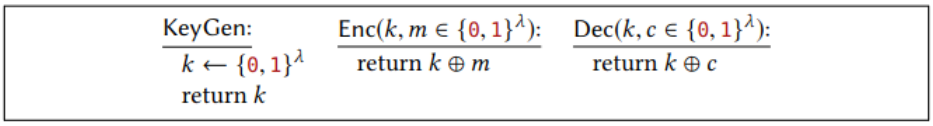
2.3 Task 3 (5 points)

We know that the plaintext word **SURFACE** is encrypted with an affine cipher into ciphertext **NJCAXTP**.

1. What is the encryption key?
2. What is the decryption key?

2.4 Task 4 (8 points)

Consider one-time-pad (OTP) encryption scheme. It is the same we discussed during practice sessions:



The plaintext m_1=**DOUGH**. The plaintext m_2=**GLORY**. Message m_1 was converted into a binary string and then encrypted using OTP with key k. The result of this encryption is ciphertext c_1=100000011000101000100100. Find the OTP encryption of m_2 with same key k.
NOTE!: The binary encoding used in this task is $A = 00000$, $B = 00001$, $C = 00010$, ..., $Z = 11001$. *Example*: the word **CAT** is 000100000010011

2.5 Bonus Task (8 points)

Consider the following encryption scheme: $c = m \wedge k$. Let's put to the side that this scheme has no decryption function defined. Does this scheme satisfy definition of perfect secrecy?