

Cryptography, ITC8240 Assignment #1

Oskar Pihlak

TalTech — October 17, 2021

Introduction

This is the Assignment #1 submission for the Cryptography course, written in LaTeX.
It's assumed that the shift cipher is defined as $C_{\alpha} = \text{ABCDEFGHIJKLMNOPQRSTUVWXYZ}$

1 Task 1: Ciphertext evaluation

Starting with plaintext $T_{\text{plain}} = \text{BLOCKCHAIN}$.

S_1 is a shift cipher with key $k_{S_1} = 9$.
All the letters in T_{plain} will be shifted by 9 characters in the alphabet.
Resulting in $T_{S_1} = \text{KUXLTLQJRW}$.

P_1 is a permutation cipher with a key $k_{P_1} = (5, 1, 3, 2, 4)$
Since k_{P_1} length is 5, T_{S_1} will be splitted into two 5 letter chunks
 $T_{S_1 \text{ chunks}} = [\text{KUXLT}, \text{LQJRW}]$
We apply the permutation cipher to each of the chunks and combine them together.
 $T_{S_1 P_1} = \text{TKXULWLJQR}$

S_2 is a shift cipher with key $k_{S_2} = 19$.
All the letters in $T_{S_1 P_1}$ will be shifted by 19 characters in the alphabet.
Resulting in $T_{S_1 P_1 S_2} = \text{MDQNE PECJK}$.

P_2 is a permutation cipher with a key $k_{P_2} = (3, 1, 4, 2, 5)$
Since k_{P_2} length is 5, $T_{S_1 P_1 S_2}$ will be splitted into two 5 letter chunks
 $T_{S_1 P_1 S_2 \text{ chunks}} = [\text{MDQNE}, \text{PECJK}]$
We apply the permutation cipher to each of the chunks and combine them together.
 $T_{S_1 P_1 S_2 P_2} = \text{QMNDE CPJEK}$

Answer: The Ciphertext is **QMNDECPJEK**

2 Task 2

Starting with plaintext $T_{\text{plain}} = \text{FRIENDSMAKETHEWORSTENEMIES}$.

1. Encrypt the plaintext using Vigenere cipher with the key $k = \text{LIST}$
The key k will repeat across the entirety of T_{plain} (24 characters) resulting in the **6k** keystream $ks = \text{LISTLISTLISTLISTLIST}$;
We will use a matrix to map the T_{plain} into the cipher values.
Resulting in $T_{\text{vignere}} = \text{QZAXYLKFLSWMSMOHCALXYMEBPA}$

	A	B	...	Z
A	A	C	...	Z
B	B	D	...	A
⋮	⋮	⋮	⋱	⋮
Z	Z	A	...	Y

2. Calculate the index of coincidence of the plaintext.
The index of coincidence can be explained with the given formula.

$$IC = \sum_{i=A}^{i=Z} \frac{n_i(n_i - 1)}{N(N - 1)}$$

All alphabet letters are looped over.
 n_i is the current letter that is being looped over.
 N is the total number of letters in the given text

$$IC(T_{plain}) = \mathbf{0.07077}$$

3. Calculate the index of coincidence of the ciphertext.
 $IC(T_{vignere}) = \mathbf{0.03692}$

3 Task 3

Starting with plaintext $T_{plain} = \mathbf{SURFACE}$ and ciphertext $T_{ciphered} = \mathbf{NJCAXTP}$.
We know that an affine cipher was used.

1. What is the encryption key?
Some of the encryption pairs are (11, 23), (37 23) and (63, 23)

2. What is the decryption key?
Some of the encryption pairs are (7, 23), (45 23) and (71, 23)

4 Task 4

Starting with plaintext $T_{plain} = \mathbf{SURFACE}$ and ciphertext $T_{ciphered} = \mathbf{NJCAXTP}$.