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} = ABCDEFGHIJKLMNOPQRSTUVWXYZ

1 Task 1: Ciphertext evaluation

Starting with plaintext T_{plain} = **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} = **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
$T_{S_1\,chunks} = [KUXLT, LQJRW]$
We apply the permutation cipher to each of the chunks and combine them together.
$T_{S_1P_1}$ = **TKXULWLJQR**

S_2 is a shift cipher with key k_{S_2} = 19.
All the letters in $T_{S_1P_1}$ will be shifted by 19 characters in the alphabet.
Resulting in $T_{S_1P_1S_2}$ = **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, $T_{S_1P_1S_2}$ will be splitted into two 5 letter chunks
$T_{S_1\,P_1\,S_2\,chunks} = [MDQNE, PECJK]$
We apply the permutation cipher to each of the chunks and combine them together.
$T_{S_1P_1S_2P_2}$ = **QMNDE CPJEK**

Answer: The Ciphertext is **QMNDECPJEK**

2 Task 2

Starting with plaintext T_{plain} = **FRIENDSMAKETHEWORSTENEMIES**.

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

	A	B	$\dots$	Z
A	A	C	$\dots$	Z
B	B	D	$\dots$	A
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
Z	Z	A	$\dots$	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}) = **0.07077**

3. Calculate the index of coincidence of the ciphertext.

IC($T_{vignere}$) = **0.03692**

3 Task 3

Starting with plaintext T_{plain} = **SURFACE** and ciphertext $T_{ciphered}$ = **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 m_1 = **DOUGH** and plaintext m_2 = **GLORY**.
Message m_1 encryption with *k* resulted in a binary ciphertext c_1 = 1000000110001010001000100. Extracting the cipher from c_1 via $\oplus$ operations gives us $cipher$ = 1001101000100010010000011. Using $cipher$ on m_2 we get the encryption c_2 = 1010100011111111010111011.

5 Task 5

We have an encryption scheme $c = m \wedge\ k$ to evaluate for perfect secrecy.
A cryptosystem has perfect secrecy if for any message x and any encipherment y, p(x|y)=p(x).
An encryption scheme is perfectly secret if the ciphertext distribution is independent from the message,
meaning every message induces the same ciphertext distribution.
The condition declared in c seems to have the message dependent in the encryption meaning the scheme is not secure.