Kabeer Ahmed SE-19028

LAB 1

Exercise:

1. Write the description of the project you are working on and encrypt it using the first letter of your name using caeser cipher.

Plain Text:

Our project is Ransomware detection and prevention that will analyze and remediation with intelligent security analytics that deliver real time actionable insight into the most critical ransomware attacks.

Key:

K → 10 (First letter of my name is K)

Cyphertext:

YEBZBYTOMDSCBKXCYWGKBONODOMDSYXKXNZBOFOXDSYXDRKDGSVVKXKVIJOKXNBOWONSKDSYXGS
DRSXDOVVSQOXDCOMEBSDIKXKVIDSMCDRKDNOVSFOBBOKVDSWOKMDSYXKLVOSXCSQRDSXDYDROW
YCDMBSDSMKVBKXCYWGKBOKDDKMUC.

2. Why rot-13 is considered an inverse of itself? Encrypt the same text twice using the same key and see the result?

ROT13 is its own inverse, because it shifts 13 letters in one time after second attempt it becomes 26 as we know that there are 26 alphabets in English language. Attempting to times rot13 will give original text.

Plain Text:

this is sample text for test

After Encryption 1 Cyphertext:

guvf vf fnzcyr grkg sbe grfg

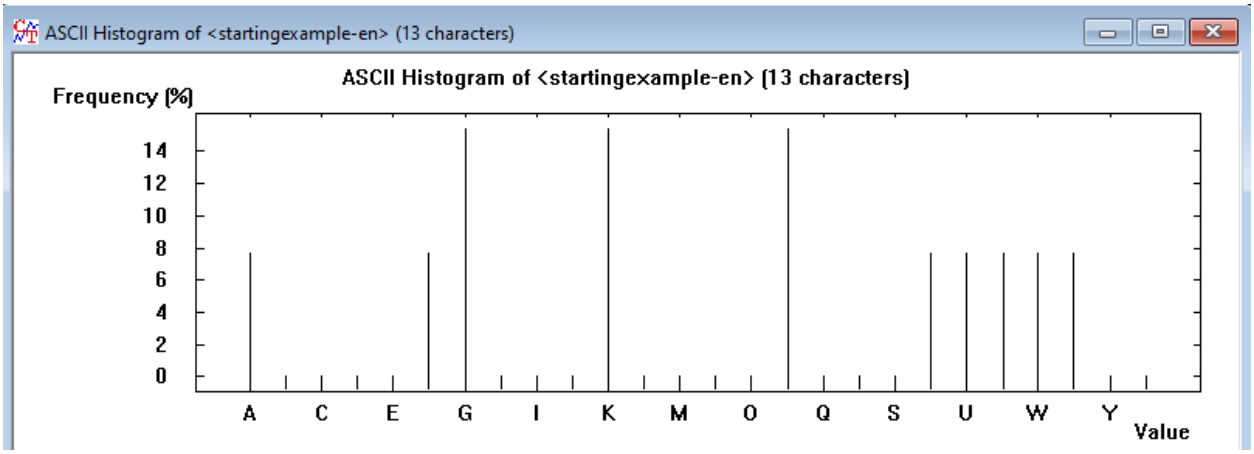
After Encryption 2 Cyphertext:

this is sample text for test

Kabeer Ahmed SE-19028

3. What does frequency analysis tell us about any encryption algorithm knowing that some letters are more common in the English language than others? How can this be used in cryptanalysis? (Break the encrypted text "pgf wpkxgtukva", what is the key? In CrypTool, run analysis->tools- >histogram)

The frequencies of letters appearing in the English language, in order from most common to least. We can use this information to help us break a code given by a Monoalphabetic Substitution Cipher. In **cryptanalysis**, frequency analysis (also known as counting letters) is the study of the frequency of letters or groups of letters in a ciphertext. The method is used as an aid to breaking classical ciphers.



4. How would you define the vigenère cipher with respect to caesar cipher where the key length is 1. Using brute force decrypt the text "ZL ANZR VF XUNA NAQ V NZ ABG N GREEBEVFG" using vigenère cipher where the key is a single letter.

Vigenère cipher uses polyalphabetic substitution while Caesar cipher is a mono alphabetic substitution. In Vigenère cipher, Vigenère table is used while in Caesar each letter is replaced by a letter some fixed number of positions down the alphabet. If the key length is taken as 1, the Vigenère cipher becomes Caesar Cipher.

Cipher Text:

ZL ANZR VF XUNA NAQ V NZ ABG N GREEBEVFG

Key:

N

Pain Text:

```
MY NAME IS KHAN AND I AM NOT A TERRORIST
```

Kabeer Ahmed SE-19028

5. What is atbash substitution, how does it work? Is the atbash a weak or strong cipher and why? If we go in to the atbash menu and select key entry: remaining characters are filed in ascending order, what is the effect of choosing a key 'LEMON' in one instance and in another instance the key 'ZXC'. Write two lines about the CSIT department of NED University and determine which key is stronger?

Atbash cipher is a substitution cipher with just one specific key where all the letters are reversed that is A to Z and Z to A. It was originally used to encode the Hebrew alphabets but it can be modified to encode any alphabet. The Atbash Cipher is a very weak substitution cipher, since there is no secret key behind generating the ciphertext alphabet to perform the encryption.

Encrypting plain text "ALPHA" with key "LEMON", the effect we get "LHPCL" as our cipher text and encrypting same plaintext with key "ZXC" we get "ZJNFZ" as our cipher text. The key which is longer i.e. "LEMON" here is stronger since the longer the key, the stronger it is.

6. Use Cryptool to analyze the cryptogram "Glh dylpo eesza jrk nxztv bzhe xkr pdmc gbk" obtained via Vigenère cipher.

Cipher Text:

Glh dylpo eesza jrk nxztv bzhe xkr pdmc gbk

Key:

NED

Pain Text:

The quick brown fox jumps over the lazy dog