Roll no. : 53
Name: Shreya Kamath
Date: 27th July, 2023.

LAB ASSIGNMENT NO. 1

AIM: Breaking Shift Cipher and Mono-alphabetic Substitution cipher using frequency analysis method.

LAB OUTCOME ATTAINED:

LO1: Illustrate symmetric cryptography by implementing classical ciphers.

THEORY:

SHIFT CIPHER

A shift cipher, also known as the Caesar cipher, is one of the simplest and oldest forms of encryption techniques. It is a substitution cipher where each letter in the plaintext is shifted a certain number of positions down the alphabet. This number is called the "key" or "shift value."

For example, with a shift value of 3, the letter "A" would be encrypted to "D," "B" to "E," and so on. The process wraps around the alphabet, so "X" would be encrypted to "A," "Y" to "B," and "Z" to "C."

The Caesar cipher can be broken using a brute-force attack because it only has 25 possible keys (shift values). With a limited number of options, an attacker can quickly try all possible shifts to decrypt the message. The lack of complexity in the cipher makes it vulnerable to this type of straightforward attack.

MONO ALPHABETIC SUBSTITUTION CIPHER:

A Monoalphabetic Substitution Cipher is a type of substitution cipher where each letter of the plaintext is replaced by a corresponding letter in the ciphertext consistently throughout the entire message. In this cipher, a fixed substitution table is used, and each letter in the plaintext is replaced by the corresponding letter in the table.

For example, if we use a monoalphabetic substitution cipher with the following table:
Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: XYZABCDEFGHIJKLMNOPQRSTUVW

Then the word "HELLO" would be encrypted as "EBIIL" using the substitution table above.
a monoalphabetic substitution cipher can be broken by a brute force attack. A brute force attack is an attempt to systematically try all possible keys until the correct one is found. In the case of a monoalphabetic substitution cipher, the key is the substitution table, which maps each letter of the alphabet to a corresponding letter in the ciphertext.

Roll no. : 53
Name: Shreya Kamath
Date: 27th July, 2023.

The reason why a brute force attack can be effective against a monoalphabetic substitution cipher is that there are only 26! (26 factorial) possible keys. Since each letter of the alphabet can be substituted with any other letter exactly once, the total number of possible keys is:
26! = 26 × 25 × 24 × ... × 3 × 2 × 1 ≈ 4.03 × 10^26
With sufficient computing power, a brute force attack can quickly test all possible keys and identify the correct one.

Frequency analysis can aid in breaking a monoalphabetic substitution cipher. Since the same plaintext letters are consistently replaced by the same ciphertext letters, patterns emerge in the frequency distribution of letters in the ciphertext. For example, the most frequent letter in the ciphertext is likely to represent the letter 'e' in the plaintext, which is the most common letter in the English language.

OUTPUT:

SHIFT CIPHER:

PART III

Plaintext:

my name is shreya

shift: 5

v Encrypt v | ^ Decrypt ^

Ciphertext

rd sfrj nx xmwjdf

Roll no. : 53
Name: Shreya Kamath
Date: 27th July, 2023.

PART III

Plaintext:

my name is shreya

shift: 10

v Encrypt v | ^ Decrypt ^

Ciphertext

wi xkwo sc crboik

MONOALPHABETIC SUBSTITUTION CIPHER:

Virtual Labs

Breaking the Mono-alphabetic Substitution Cipher

PART II

Note that the *cipher text is in lower case* and when you replace any character, the final character of replacement, i.e., *plaintext is changed to upper case* automatically in the following scratchpad.

Scratchpad:

dkxyvrh 1 - qegt vkr hxccwv keur: xuwdr wn cehrq nwvvwtp et vkr hwsrhcxto gwvk krh nwnvrh, gkrt nkr tevwdrn x vxuowtp, duevkrq gkwvr hxccwv gwvk x vedorv gxvdk hit yxnv. nkr leuuegn wv qegt x hxccwv keur gkrt niqqrtub nkr lxuun x uetp gxb ve x dihwein kxuu gwvk fxtb uedorq qeehn el xuu nwmrn. nkr lwtqn x nfxuu orb ve x qeeh vee nfxuu leh krh ve lwv, civ vkheipk gkwdk nkr nrrn xt xvvhxdvwsr pxhqrt. nkr vkrt qwndesrhn x cevvuc uxcruurq 'ghwto fr', vkr detvrtvn el gkwdk dxinr krh ve nkhwto vee nfxuu ve hrxdk vkr orb. x dxor gwvk 'rxv fr' et wv dxinrn krh ve pheg ve nidk x vhrfrtqein nwmr krh krxq kwvn vkr drwuwtp.

Modify the text above (in scratchpad):

This is case *insensitive* function and replaces only cipher text (lower case) by plain text (upper case):

Replace cipher character [ ] by plaintext character [ ] Modify

Use the following function to undo any unwanted exchange by giving an uppercase character and a lower case. This is a case sensitive function:

Replace character [ ] by character [ ] Replace these exact characters

Your replacement history:

Roll no. : 53
Name: Shreya Kamath
Date: 27th July, 2023.

Virtual Labs

Breaking the Mono-alphabetic Substitution Cipher

Note that the *cipher text is in lower case* and when you replace any character, the final character of replacement, i.e., *plaintext is changed to upper case* automatically in the following scratchpad.

Scratchpad:

```
YTxyvrQ 1 - qVHt vTr QxXXwv TVur: xuwYr wn XVQrq nwvvwtp Vt vTr
QwsrQXxto HwvT TrQ nwnvrQ, HTrt nTr tVvwYrn x vxuowtp, YuVvTrq HTwvr
QxXXwv HwvT x yVYorv HxvYT QEt yxnv. nTr WVuuVHn wv qVHt x QxXXwv TVur
HTrt nEqqrtuK nTr Wxuun x uVtp HxK vV x YEQwVEn Txuu HwvT RxtK uVYorq
qVVQn VW xuu nwmrn. nTr Wwtqn x nRxuu orK vV x qVVQ vVV nRxuu WVQ TrQ vV
Wwv, XEv vTQVEpT HTwYT nTr nrrn xt xvvQxYvwsr pxQqrt. nTr vTrt qwnYVsrQn
x XVvvur uxXruurq 'qQwto Rr', vTr YVtvrtvn VW HTwYT YxEnr TrQ vV nTQwto
vVV nRxuu vV QrxYT vTr orK. x Yxor HwvT 'rxv Rr' Vt wv YxEnrn TrQ vV
pQVH vV nEYT x vQrRrtqVEn nwmr TrQ Trxq Twvn vTr Yrwuwtp.
```

Modify the text above (in scratchpad):

This is case *insensitive* function and replaces only cipher text (lower case) by plain text (upper case):

Replace cipher character [1] by plaintext character [W] Modify

Use the following function to undo any unwanted exchange by giving an uppercase character and a lower case. This is a case sensitive function:

Replace character [ ] by character [ ] Replace these exact characters

Your replacement history:

You replaced a by D You replaced a by D You replaced b by K You replaced c by X You replaced d by Y You replaced e by V You replaced f by R You replaced g by H You replaced h by Q You replaced i by E You replaced j by Q You replaced j by U You replaced k by T You replaced l by W

PART IV

Plaintext

```
welcome to the mystery text: when we speak plainly of
the mysteries which are ever around, both our spoken
and written words can lead us astray. but knowing a
mystery does not trouble the tongue as knowing a lie
does not trouble our mind. but these great many years
we have been told of this lie by those whom we trusted
most. but surely we must trust 'the one who', the
creator of all things. the next chapter in history is
```

key = wjexcvtqkurmnopqglvwfxdyzs Generate Random Key

v Encrypt v ^ Decrypt ^

☐ Remove Punctuation

Ciphertext

```
dcmepnc wp wqc nzvwclz wcyw: dqco dc vqcwr qmwkomz
pv wqc nzvwclkcv dqkeq wlc cxcl wlpfox, jpwq pfl
vqprco wox dlkwwco dplxv ewo mcwx fv wvwlwz. jfw
ropdkot w nzvwclz xpcv opw wlpfjmc wqc wpotfc wv
ropdkot w mkc xpcv opw wlpfjmc pfl nkox. jfw wqcvc
tlcww nwoz zcwlv dc qwxc jcco wpmx pv wqkv mkc jz
```

CONCLUSION:

Hence, we have illustrated symmetric cryptography by implementing classical ciphers like the shift cipher and mono-alphabetic substitution cipher.