

Roll Number:- 2105048

Name:-Manav Jain

Date:- 19/07/2023

Lab Assignment No:-1

Aim:- Breaking Shift Cipher and Monoalphabetic substitution cipher using frequency analysis method.

Lab Outcome Attained :- LO1

Theory:-

What is Shift Cipher ? (with eg)

One of the earliest and most basic cryptosystems is the shift cipher. Each letter in a given plaintext is moved n positions in order to encrypt it into a ciphertext. An illustration of how to encrypt plaintext by shifting each letter three times.

Shift cipher is simple in plaintext.

Ciphertext: X be the position number of a letter from the alphabet (vkliwflskhulvvlpsoh).

The key for the shift cipher cryptosystem's encryption and decryption is an integer in the range 0 to 25.

The encryption process is (the x here represents a letter from plaintext):
 $x+n \pmod{26}$

The decryption process is (the x here represents a letter from ciphertext):

$x - n \pmod{26}$

How and why shift cipher can be broken using Brute force attack ?

A brute force assault is a technique for decrypting data that involves testing every key until the plaintext is exposed. There are only 26 possible keys for a shift cipher, making it extremely simple to carry out a brute force attack.

A brute force assault would encrypt the ciphertext with each of the 26 potential keys in order to crack a shift cipher. The attacker would be able to determine which key was the right one once the plaintext had been disclosed.

For instance, the plaintext would be "hello" if the ciphertext was "FEQJP" and the shift was 3. To get "hello" as the plaintext, the attacker would simply encrypt the ciphertext with each of the 26 potential keys.

What is monoalphabetic cipher ?(with eg)

Each letter in the plaintext is mapped to a single letter of the ciphertext in a monoalphabetic cipher, a form of substitution cipher. This indicates that the plaintext's letters and the ciphertext's letters are identical to one another.

A straightforward monoalphabetic cipher called the Caesar shifts each letter in the plaintext by a predetermined number of places. For instance, if the shift is 3, the letters A and B would be encoded as D and E, respectively.

The Caesar cipher would function as shown in the following example:

Plaintext: HELLO Key: 3 Ciphertext: KILO

To decrypt the ciphertext, simply shift each letter back by the same number of positions. In this case, you would shift each letter back 3 positions. Ciphertext: KILO Key: 3 Plaintext: HELLO

Can monoalphabetic cipher broken using brute force attack ? Why ?

No, due to its huge keyspace, monoalphabetic ciphers cannot be cracked using brute force methods. The set of all potential keys that might be used to encrypt a message is known as the keyspace of a monoalphabetic cipher. A simple permutation of the alphabet serves as the key in a monoalphabetic cipher. This indicates that a monoalphabetic cipher with a 26-letter alphabet has $26!$ potential keys.

Monoalphabetic ciphers can be cracked via frequency analysis.

How can it be broken using frequency analysis attack ?

Frequency analysis is a cryptanalysis technique that exploits the fact that certain letters are more common than others in a language. For example, the letter "E" is the most common letter in the English language, followed by "T" and "A". This means that if you know the frequency of letters in the plaintext, you can use frequency analysis to guess the key of the ciphertext.

To break a monoalphabetic cipher using frequency analysis, you would first need to create a

frequency table of the letters in the ciphertext. This table would show how often each letter appears in the ciphertext. Once you have created the frequency table, you would then need to compare it to the frequency table of the plaintext.

If the two frequency tables are similar, then you can use the frequency table of the plaintext to guess the key of the ciphertext. For example, if the letter "E" appears most often in the ciphertext, then you can guess that the letter "E" in the plaintext is mapped to the letter "E" in the ciphertext. This procedure can be repeated and then ciphertext can be converted to plain text .

Output Screenshot:-

1)breaking the shift cipher

Virtual Labs

Breaking the Shift Cipher

Ciphertext to be decrypted:

haahjr ha khdu

Next Ciphertext

PART II

Do your rough work here:

0:haahjr ha khdu
1:gzzgla gz tact
2:fyfthp fy ifbz
3:exxogo ex hear
4:dwdfrn dw gdza
5:cvvcem cv fcyo
6:buubdl bu sbzo
7:attack at dawn

PART III

Plaintext:

attack at dawn

shift: 7

Encrypt Decrypt

Ciphertext

haahjr ha khdu



Breaking the Shift Cipher

Ciphertext to be decrypted:

wkh srufxslah lv xaghu wkh vkhhuv

Next Ciphertext

PART II

Do your rough work here:

0: wkh srufxslah lv xaghu wkh vkhhuv
1: vjg rufxslah lv xaghu wkh vkhhuv
2: uif srufxslah lv xaghu wkh vkhhuv
3: the porcupine is under the sheets

PART III

Plaintext:

the porcupine is under the sheets

shift: 3

Encrypt Decrypt

Ciphertext

wkh srufxslah lv xaghu wkh vkhhuv

PART III

Plaintext:

attack at dawn



shift: 7 ▼

↻ Encrypt ↻

^ Decrypt ^

Ciphertext

haahjr ha khdu



PART IV

Enter your solution Plaintext and shift key here:

attack at dawn



Key 7 ▼

Check my answer!

CORRECT!!



PART III

Plaintext:

the porcupine is under the sheets

shift: 3 ▼

⌵ Encrypt ⌵

⌶ Decrypt ⌶

Ciphertext

wkh srufxslqh lv xgghu wkh vkhhwv

PART IV

Enter your solution Plaintext and shift key here:

the porcupine is under the sheets

Key 3 ▼

Check my answer!

CORRECT!!

2)breaking the monoalphabetic substitution cipher - Q1



Breaking the Mono-alphabetic Substitution Cipher

PART I

Decrypt the following cipher text. A tool to simulate the Mono-Alphabetic Substitution cipher is provided beneath for your assistance.

Here is the table of frequencies of English alphabets for your reference:

a	b	c	d	e	f	g	h	i	j	k	l	m
8.167	1.49	2.782	4.253	12.702	2.228	2.015	6.094	6.966	0.153	0.772	4.025	2.406
n	o	p	q	r	s	t	u	v	w	x	y	z
6.749	7.507	1.929	0.095	5.987	6.327	9.056	2.758	0.978	2.360	0.150	1.974	0.074

dkoxyrh i - qegt vkr hxcvur keur: xuadr un cehrq mrvvutp et vkr
husrhcxto gwvk krh mrvvrh, gkrt nkr tevadrn x vxuowtp, duevkrg klwvr
hxcvur gwvk x yedovr gvxvk hlt yxnv, nkr leuegn vr degt x hxcvur keur
gkrt nqqrutub nkr lxuun x uetp gxb ve x dluweln lxuun gwvk fxtb uedorg
qeehn el xuu nmrm. nkr lutqn x nfxuu orb ve x qeeh vee nfxuu leh krh
ve lwr, civ vkheipk glwvdk nkr nrm xt xvvhxvdrp pxdqrt. nkr vkrt

Next Ciphertext

Calculate Frequencies in ciphertext

Ciphertext Frequencies:

a	b	c	d	e	f	g	h	i	j	k	l	m
0.000	1.037	2.282	3.942	8.091	1.452	3.112	5.602	2.075	0.000	8.506	1.452	0.415
n	o	p	q	r	s	t	u	v	w	x	y	z
7.469	1.867	1.452	3.32	11.618	0.622	4.979	5.602	9.959	6.639	7.884	0.622	0.000



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:

CHAPTER 1 - DOWN THE RABBIT HOLE: ALICE IS BORED SITTING ON THE RIVERBANK WITH HER SISTER, WHEN SHE NOTICES A TALKING, CLOTHED WHITE RABBIT WITH A POCKET WATCH RUN PAST. SHE FOLLOWS IT DOWN A RABBIT HOLE WHEN SUDDENLY SHE FALLS A LONG WAY TO A CURIOUS HALL WITH MANY LOCKED DOORS OF ALL SIZES. SHE FINDS A SMALL KEY TO A DOOR TOO SMALL FOR HER TO FIT, BUT THROUGH WHICH SHE SEES AN ATTRACTIVE GARDEN. SHE THEN DISCOVERS A BOTTLE LABELLED 'DRINK ME', THE CONTENTS OF WHICH CAUSE HER TO SHRINK TOO SMALL TO REACH THE KEY. A CAKE WITH 'EAT ME' ON IT CAUSES HER TO GROW TO SUCH A TREMENDOUS SIZE HER HEAD HITS THE CEILING.

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

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

Replace character by character

Your replacement history:

You replaced x by A You replaced e by B You replaced d by C You replaced q by D You replaced r by E You replaced i by F You replaced p by G You replaced k by H You replaced w by I You replaced z by J You replaced o by K You replaced u by L You replaced f by M You replaced t by N You replaced v by O You replaced y by P You replaced a by Q You replaced h by R You replaced n by S You replaced v by T You replaced s by U You replaced a by V You replaced g by W You replaced j by X You replaced b by Y You replaced m by Z

PART III

Enter your solution plaintext here:


CHAPTER 1 - DOWN THE RABBIT HOLE: ALICE IS BORED SITTING ON THE RIVERBANK WITH HER SISTER, WHEN SHE NOTICES A TALKING, CLOTHED WHITE RABBIT WITH A POCKET WATCH RUN PAST. SHE FOLLOWS IT DOWN A RABBIT HOLE WHEN SUDDENLY SHE FALLS A LONG WAY TO A CURIOUS HALL WITH MANY LOCKED DOORS OF ALL SIZES. SHE FINDS A SMALL KEY TO A DOOR TOO SMALL FOR HER

Solution Key =

CORRECT!!



3)breaking the monoalphabetic substitution cipher - Q2



Breaking the Mono-alphabetic Substitution Cipher

PART I

Decrypt the following cipher text. A tool to simulate the Mono-Alphabetic Substitution cipher is provided beneath for your assistance.


Here is the table of frequencies of English alphabets for your reference:

a	b	c	d	e	f	g	h	i	j	k	l	m
8.167	1.49	2.782	4.253	12.702	2.228	2.015	6.094	6.966	0.153	0.772	4.025	2.406
n	o	p	q	r	s	t	u	v	w	x	y	z
6.749	7.507	1.929	0.095	5.987	6.327	9.056	2.758	0.978	2.360	0.150	1.974	0.074

zelpjxp. zex rpxagz lnn jhl obxixz npld jex dkzeplld. lfx zbux dagxz exp zepbfg zdawoxp jeaf xcxp, hebvx afljexp iakxzx exp fxig jl mpla ebme bfil jex jpxxz, hexpx a obmelf dbzjagxz exp nlp a zpxoxfj. hbje zldx xnnlpj, awbix rpbfmz expzxon raig jl exp kzkaw exbmej. zex zjkdrwxz kolf a zdaww xzjaix afu kxzx jex dkzeplld jl pxaie a dlpw aoplopbaix exbmej.

Ciphertext Frequencies:

a	b	c	d	e	f	g	h	i	j	k	l	m
8.084	6.854	0.176	4.394	7.206	4.394	1.757	1.582	2.988	7.909	2.636	7.381	1.582
n	o	p	q	r	s	t	u	v	w	x	y	z
1.582	2.285	8.26	0.000	1.582	0.000	0.703	1.933	0.000	5.097	14.06	0.176	7.381



Virtual Labs
For World-Class and Innovative Education

Breaking the Mono-alphabetic Substitution Cipher

PART III

Enter your solution plaintext here:

ALICE COMES UPON A MUSHROOM AND SITTING ON IT IS A BLUE CATERPILLAR
SMOKING A HOOKAH. THE CATERPILLAR QUESTIONS ALICE AND SHE ADMITS TO
HER CURRENT IDENTITY CRISIS, COMPOUNDED BY HER INABILITY TO REMEMBER A
POEM. BEFORE CRAWLING AWAY, THE CATERPILLAR TELLS ALICE THAT ONE SIDE
OF THE MUSHROOM WILL MAKE HER TALLER AND THE OTHER SIDE WILL MAKE HER

Solution Key =

CORRECT!!

Conclusion:-

used symmetric cryptography on some random plain text to create shift cipher and monoalphabetic substitution cipher, learning more about how it works in the process.

