Experiment 1

Aim:

To understand the process of Breaking the Mono-alphabetic Substitution Cipher using Frequency analysis method.

Theory:

A mono-alphabetic cipher is a substitution cipher where each letter of the plain text is replaced with another letter of the alphabet. It uses a fixed key which consists of the 26 letters of a "shuffled alphabet". Spaces and punctuation are left as it is.
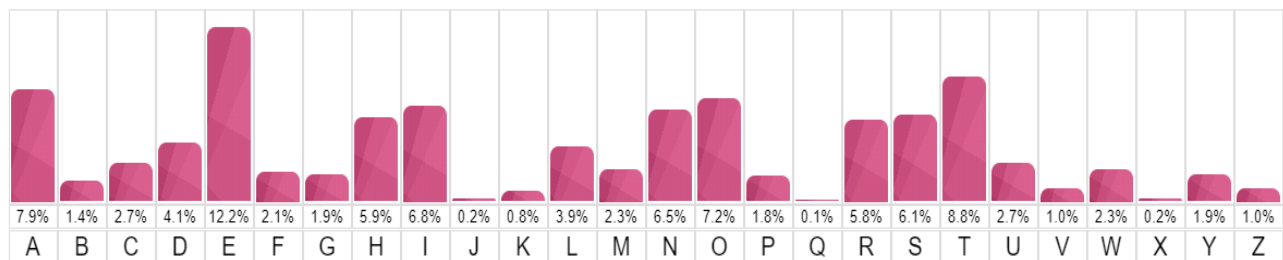
Algorithm-
1. We first count the number of letters in cipher text and find the frequency of each letter.
2. Then we compare the frequency of letters of cipher text and plain text.
3. We then substitute the letters of cipher text which have the same frequency as plain text.

Output -

The following chart shows the frequency of each letter of the alphabet for the English language.

The following chart shows the frequency of each letter of the alphabet for the English language:

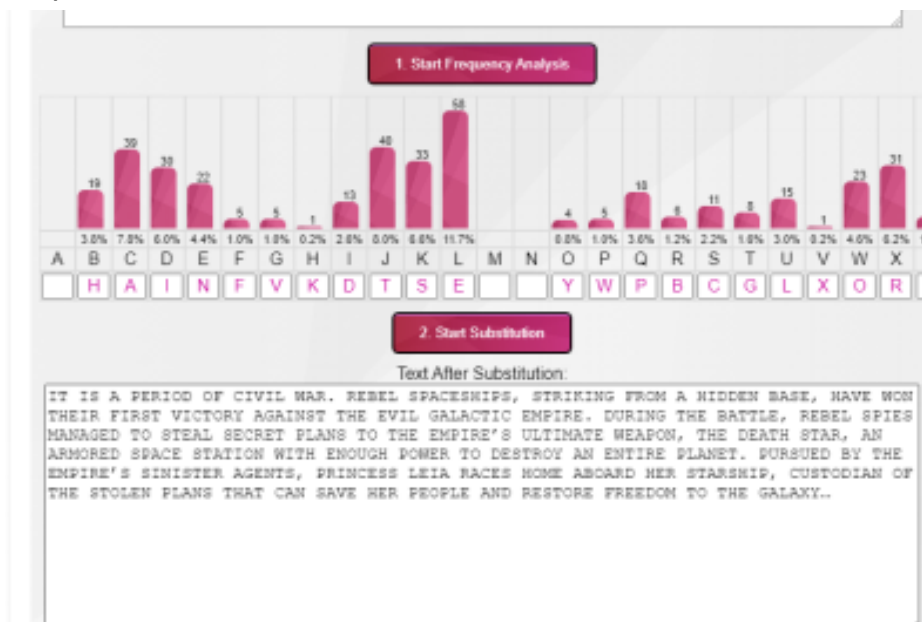| A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7.9%	1.4%	2.7%	4.1%	12.2%	2.1%	1.9%	5.9%	6.8%	0.2%	0.8%	3.9%	2.3%	6.5%	7.2%	1.8%	0.1%	5.8%	6.1%	8.8%	2.7%	1.0%	2.3%	0.2%	1.9%	1.0%

We can assume that most samples of text written in English would have a similar distribution of letters. However this is only true if the sample of text is long enough. A very short text may lead to a significantly different distribution.

Cipher Text 1-

Text:

DJ DK C QLXDWI WF SDGDU PCX. XLRLU KQCSLKBDQK, KJXDHDET FXWZ C BDIILE RCKL, BCGL
PWE JBLDX FDXKJ GDSJWXO CTCDEKJ JBL LGDU TCUCSJDS LZQDXL. IYXDET JBL RCJJUL,
XLRLU KQDLK ZCECTLI JW KJLCU KLSXLJ QUCEK JW JBL LZQDXL'K YUJDZCJL PLCQWE, JBL
ILCJB KJCX, CE CXZWXLI KQCSL KJCJDWE PDJB LEWYTB QWPLX JW ILKJXWO CE LEJDXL
QUCELJ. QYXKYLI RO JBL LZQDXL'K KDEDKJLX CTLEJK, QXDESLKK ULDC XCSLK BWZL CRWCXI
BLX KJCXKBDQ, SYKJWIDCE WF JBL KJWULE QUCEK JBCJ SCE KCGL BLX QLWQUL CEI XLKJWXWL
FXLLIWZ JW JBL TCUCVO…

Deciphered text-

1. Start Frequency Analysis

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
Count	19	39	30	22	5	5	1	13	48	33	68			4	5	13	8	11	8	15	1	23	31		
%	3.0%	7.0%	6.0%	4.4%	1.0%	1.0%	0.2%	2.6%	0.0%	6.6%	11.7%			0.0%	1.0%	3.0%	1.2%	2.2%	1.0%	3.0%	0.2%	4.0%	6.2%	1.2%	
Sub		H	A	I	N	F	V	K	D	T	S	E			Y	W	P	B	C	G	L	X	O	R	U

2. Start Substitution

Text After Substitution:

IT IS A PERIOD OF CIVIL WAR. REBEL SPACESHIPS, STRIKING FROM A HIDDEN BASE, HAVE WON
THEIR FIRST VICTORY AGAINST THE EVIL GALACTIC EMPIRE. DURING THE BATTLE, REBEL SPIES
MANAGED TO STEAL SECRET PLANS TO THE EMPIRE'S ULTIMATE WEAPON, THE DEATH STAR, AN
ARMORED SPACE STATION WITH ENOUGH POWER TO DESTROY AN ENTIRE PLANET. PURSUED BY THE
EMPIRE'S SINISTER AGENTS, PRINCESS LEIA RACES HOME ABOARD HER STARSHIP, CUSTODIAN OF
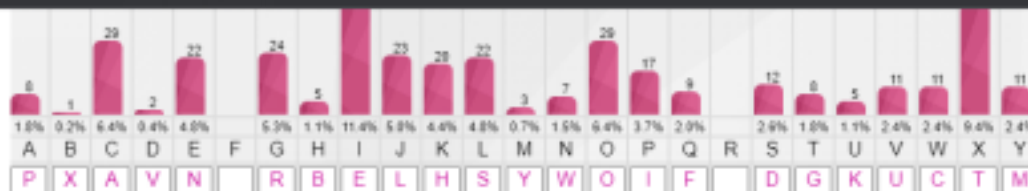THE STOLEN PLANS THAT CAN SAVE HER PEOPLE AND RESTORE FREEDOM TO THE GALAXY…

Cipher Text 2-

Text:

```
JVUI LUMNCJUIG KCL GIXVGEIS XO KPL KOYI AJCEIX OQ XCXOOPEI PE CE CXXIYAX XO
GILWVI KPL QGPIES KCE LOJO QGOY XKI WJVXWKIL OQ XKI DPJI TCETLXIG BCHHC XKI
KVXX.
JPXXJI SOIL JVUI UEON XKCX XKI TCJCWXPW IYAPGI KCL LIWGIXJM HITVE WOELXGVWXPOE
OE C EIN CGYOGIS LACWI LXCXPOE IDIE YOGI AONIGQVJ XKCE XKI QPGLX SGICSIS SICXK
LXCG.
NKIE WOYAJIXIS, XKPL VJXPYCXI NICAOE NPJJ LAIJJ WIGXCPE SOOY QOG XKI LYCJJ HCES
OQ GIHIJL LXGVTTJPET XO GILXOGI QGIISOY XO XKI TCJCZM…
```

Deciphered text-

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
1.8%	0.2%	6.4%	0.4%	4.0%		6.3%	1.1%	11.4%	5.8%	4.4%	4.8%	0.7%	1.5%	6.4%	3.7%	2.0%		2.9%	1.8%	1.1%	2.4%	2.4%	9.4%	2.4%
P	X	A	V	N		R	B	E	L	H	S	Y	W	O	I	F		D	G	K	U	C	T	M

2. Start Substitution

Text After Substitution:

```
LUKE SKYWALKER HAS RETURNED TO HIS HOME PLANET OF TATOOINE IN AN ATTEMPT TO
RESCUE HIS FRIEND HAN SOLO FROM THE CLUTCHES OF THE VILE GANGSTER XABBA THE
HUTT.
LITTLE DOES LUKE KNOW THAT THE GALACTIC EMPIRE HAS SECRETLY BEGUN CONSTRUCTION
ON A NEW ARMORED SPACE STATION EVEN MORE POWERFUL THAN THE FIRST DREADED DEATH
STAR.
WHEN COMPLETED, THIS ULTIMATE WEAPON WILL SPELL CERTAIN DOOM FOR THE SMALL BAND
OF REBELS STRUGGLING TO RESTORE FREEDOM TO THE GALAXY…
```

Cipher text 3-

Text:

```
OK OH R WRFD KOIS QPF KNS FSTSJJOPX. RJKNPAGN KNS WSRKN HKRF NRH TSSX WSHKFPCSW,
OIBSFORJ KFPPBH NRYS WFOYSX KNS FSTSJ QPFMSH QFPI KNSOF NOWWSX TRHS RXW BAFHASW
KNSI RMFPHH KNS GRJREC.
SYRWOXG KNS WFSRWSW OIBSFORJ HKRFQJSSK, R GFPAB PQ QFSSWPI QOGNKSFH JSW TC JADS
HDCVRJDSF NRH SHKRTJOHNSW R XSV HSMFSK TRHS PX KNS FSIPKS OMS VPFJW PQ NPKN.
KNS SYOJ JPFW WRFKN YRWSF, PTHSHHSW VOKN QOXWOXG CPAXG HDCVRJDSF, NRH WOHBRKMNSW
KNPAHRXWH PQ FSIPKS BFPTSH OXKP KNS QRF FSRMNSH PQ HBRMS…
```

Deciphered text-

Conclusion-

Thus we have successfully deciphered text which was ciphered using mono-alphabetic substitution.