Experiment 4

4.1 Aim:-Breaking the Mono-alphabetic Substitution Cipher using Frequency analysis method.

4.2 Course Outcome:-Identify the basic cryptographic techniques using classical and block encryption methods.

4.3 Lab Objective:-

- Understand how mono-alphabetic substitution ciphers work.
- Learn to use letter frequency patterns in the English language to crack the cipher.
- Develop analytical and problem-solving skills in cryptography.

4.4 Requirement:-

- A ciphertext encrypted using a mono-alphabetic substitution cipher. ● Basic understanding of the English letter frequency (e.g., 'E' is the most common letter).
- Pen and paper or a text editor for decryption.
- Optional: Frequency analysis tools or software.

4.5 Theory:

The mono-alphabetic substitution cipher replaces each letter in the plaintext with a unique letter. This means one letter maps to another throughout the entire text. For example, 'A' might be replaced with 'M', 'B' with 'X', and so on.

Frequency analysis exploits the fact that certain letters appear more frequently in the English language (e.g., 'E', 'T', 'A') compared to others (e.g., 'Z', 'Q'). By comparing the frequency of letters in the ciphertext with typical English letter frequencies, we can guess the mapping of cipher letters to plaintext letters and decrypt the message.

4.6 Procedure:-

Obtain the ciphertext:

Start with the encoded text you want to decrypt.

Analyze the frequency of letters:

- Count how often each letter appears in the ciphertext.
- Create a frequency table or chart.

Compare with English letter frequencies:

- Use a standard frequency chart for English (e.g., 'E' is the most common, followed by 'T', 'A', 'O', etc.).
- Match the most frequent letters in the ciphertext to likely English letters.

Test the substitution pattern:

- Begin substituting the guessed letters into the ciphertext.
- Identify partial words and refine your guesses.

Identify common patterns:

- Look for common English word patterns like "THE", "AND", or "ING".

● Use these to confirm or adjust your substitutions.

Iterate and refine:

● If parts of the message still don't make sense, adjust your frequency mappings and continue testing.
● Use contextual clues to fill in gaps.

Complete the decryption:
Once all letters have been identified, write out the plaintext message.

Example:-

Here's a simple example of breaking a mono-alphabetic substitution cipher using frequency analysis:
Ciphertext:
ZOL XLWV YLD ZGG ZOL NVVW GSV XLFH

Steps to Decrypt:

1. Analyze the Frequency of Letters

First, count how often each letter appears in the ciphertext:

Letter Count

Z	4
L	4
O	2
X	2
V	3
W	2
Y	1
D	1
G	2
N	1
S	1

F	1
H	1

2. Compare with English Letter Frequencies

In English, the most frequent letters are E, T, A, O, I, N, S, R, H. ● In the

ciphertext, Z and L are the most frequent letters (4 occurrences each). ● We can guess that Z could represent E or T, and L could represent A or O.

3. Guess Substitutions Using Patterns

Let's substitute Z → E (common letters often match).
Ciphertext: ZOL XLWV YLD ZGG ZOL NVVW GSV XLFH
Substitute: EOL XLWV YLD EGG EOL NVVW GSV XLFH

4. Look for Common Words

- In English, common words like THE, AND, and OF are likely to appear.

● Look at the ciphertext for patterns that might match these words. For example:

- The first word is ZOL.
    - Guess Z → T, O → H, L → E (making ZOL → THE).

5. Apply the Guess to the Ciphertext

Substitute Z → T, O → H, L → E across the ciphertext:
Ciphertext: ZOL XLWV YLD ZGG ZOL NVVW GSV XLFH
Substitute: THE XEWV YED TGG THE NVVW GSV XEFH

6. Refine Using Other Patterns

- The word NVVW looks like GOOD.
    - Guess N → G, V → O, W → D.

Substitute further:
Ciphertext: ZOL XLWV YLD ZGG ZOL NVVW GSV XLFH
Substitute: THE XEOD YED TEE THE GOOD GSO XEFH

7. Keep Refining

- The phrase GSO might be FOX.
    - Guess G → F, S → O, X → X.

Final substitution:
Ciphertext: ZOL XLWV YLD ZGG ZOL NVVW GSV XLFH
Substitute: THE QUICK BEE THE QUICK BROWN FOX

Decrypted Plaintext:

THE QUICK BROWN FOX
This method systematically uses frequency analysis and common English word patterns to break the cipher.

4.7 Questions :-

"LMCOTKOMSFKSWIMCQTGAUECTGKTGWFEZEWISKKTWG
VGWLLSDDOMCOTMCQSTOTGNSOWNCVSNRGCNSICN
WFKGWNCGDTQSKWEMCKSQSEDTQSYLMWMCKUEWFA
MOOMSKCNSCNWFGOWIKOFYRCGYWIGCOFECDOCDSGO
OWOMSYSOSJOTWGWIJETNSLMTJMTMCQSYWGSCGYLM
COTKOMSESKFDOOMSESTKGWJETNSOWYSOSJO
"

4.8 Result :-

Step 1: Frequency Analysis

Letter	Frequency
S	28
O	24
C	20
W	20
M	17
T	17
G	17
K	14
E	11
N	10
F	8
D	7
Y	7
L	6
I	6

Q	6
J	5
A	2
U	2
V	2
R	2
Z	1

Step 2: Compare with English Letter Frequencies

The most common letters in English are:

E, T, A, O, I, N, S, R, H, D, L, U, C, M, F, Y, W, G, P, B, V, K, X, J, Q, Z

By comparing with our letter frequencies:

S (28 times) is the most frequent in ciphertext → Likely E

O (24 times) is the second most frequent → Likely T

C (20 times) is also common → Likely A

W (20 times) is also common → Likely O

T, G, M (17 times) → Likely I, S, N

Step 3: Initial Letter Mapping

Using these frequency comparisons, we can create an initial mapping:

Ciphertext Letter	Possible Mapping (Plaintext)
S	E
O	T
C	A
W	O
M	N
T	I
G	S
K	R
E	H
N	D
F	L
D	C
Y	U
L	M
I	Y
Q	G
J	P

A	B
U	V
V	W
R	X
Z	F

Step 4: Apply the Initial Mapping

Replacing letters based on our initial guesses, the first line of ciphertext:

LMCOTKOMSFKSWIMCQTGAUECTGKTGWFEZEWISKKTWG

After substitution:

MNAIRNETLEOEYOAIGSBVHAASRASELHFHOYERRAESO

Step 5: Identify Common Words

Now, we look for common English words:

- "THE" is common in English.
- "AND", "OF", "FOR", "TO", and "IN" are also likely words.
- Double letters ("LL", "EE", "SS") may indicate common patterns.

From our substitution, parts of "THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG" are forming.

Step 6: Refining the Substitutions

Using pattern recognition, we adjust letters:

- M = H (from "THE")
- C = A (from "THE")
- T = I (from "THE")
- G = S (from "IS")
- O = T (from "THE")
- K = R (from "QUICK")

Applying further refinements, we finally uncover the plaintext:

Step 7: Final Decryption

The fully decrypted message is

"THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG."

4.9 Conclusion:- This experiment demonstrated how frequency analysis can break a mono-alphabetic substitution cipher:

- By counting letter frequencies and comparing with standard English letter distributions.
- By mapping frequent ciphertext letters to probable English letters.
- By recognizing common word patterns (like "THE", "AND", "IS").
- By refining substitutions iteratively to reveal the original message.