Practical No. 1

Aim: Breaking the mono alphabetic cipher using frequency and analysis method.

Theory:

Breaking a Monoalphabetic Cipher Using Frequency Analysis is a classic cryptanalysis technique used when a message is encrypted with a substitution cipher where each letter in the plaintext is replaced by another fixed letter from the alphabet.

What is a Monoalphabetic Cipher?

A **monoalphabetic substitution cipher** replaces each letter of the plaintext with a corresponding letter of ciphertext using a single substitution key. For example:

Plain: A B C D E ...
Cipher: Q W E R T ...

This means 'A' is always replaced with 'Q', 'B' with 'W', etc.

Steps to Break a Monoalphabetic Cipher Using Frequency Analysis

Step 1: Collect the Ciphertext

Start with the encrypted message.
Example:

Ciphertext: GSV XLWV RH Z HVXIVG NVHHZTV

Step 2: Count Letter Frequencies

Calculate how often each letter appears in the cipher text.

Step 3: Match Frequencies

Make a substitution guess based on frequency match.

(English typical frequencies): **"ETAON RISHD LFCMU GYPWB VKJXZQ"**

If 'V' is most common in the ciphertext and 'E' is most common in English, assume:

V	E

And so on for other common letters:

H	T
G	A
S	O
...	

Step 4: Identify Common Words and Patterns

Look for frequent 1-letter and 3-letter words:

- 1-letter: 'A', 'I'
- 2-letter: "is", "to", "of", "it", etc.
- 3-letter: "the", "and", "you", etc.

Try substitutions in the ciphertext to guess possible words.

Step 5: Refine the Key

With some guesses in place, refine the mapping by trial and error:

- Replace guessed letters in the ciphertext
- See if intelligible words form
- Adjust assumptions as needed

Step 6: Decrypt the Ciphertext

Once the full or partial substitution key is known, decrypt the entire message.

Example Using Atbash Cipher (Simple Monoalphabetic)

Let’s decode this using **Atbash cipher**, where:

```
A  Z, B  Y, C  X, ..., M  N
```

Ciphertext:

```
GSV XLWV RH Z HVXIVG NVHHZTV
```

Applying Atbash:

```
THE CODE IS A SECRET MESSAGE
```

So:

```
Decrypted: THE CODE IS A SECRET MESSAGE
```