DOP: / /2023 **DOS: / /2023**

Experiment No: 01

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

Theory:

- **Cryptography**

Cryptography is technique of securing information and communications through use of codes so that only those people for whom the information is intended can understand it and process it. Thus, preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graph means "writing"

Plaintext can refer to anything which humans can understand and/or relate to. This may be as simple as English sentences, a script, or Java code. If you can make sense of what is written, then it is in plaintext.

Ciphertext, or encrypted text, is a series of randomized letters and numbers which humans cannot make any sense of. An encryption algorithm takes in a plaintext message, runs the algorithm on the plaintext, and produces a ciphertext. The ciphertext can be reversed through the process of decryption, to produce the original plaintext.

There are two basic building blocks of all encryption techniques:

- SUBSTITUTION TECHNIQUES
- TRANSPOSITION TECHNIQUES

⚫Substitution Techniques:

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

⚫Mono-alphabetic Substitution Cipher:

The mono-alphanumeric substitution cipher is the oldest forms of encryption algorithms according to creates each character of a plaintext message and require a substitution process to restore it with a new character in the ciphertext.

Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if 'A' is encrypted as 'D', for any number of occurrences in that plaintext, 'A' will always get encrypted to 'D'.

All of the substitution ciphers we have discussed earlier in this chapter are monoalphabetic; these ciphers are highly susceptible to cryptanalyst.

⚫ALGORITHM

- STEP-1: Read the plain text from the user.
- STEP-2: Read the plan text position from the user.
- STEP-3: comparing the character and adding the corresponding char to the encrypted String STEP-4: Run the for loop for total string.
- STEP-5: Display the cipher text obtained above.

Input :

```
// Java Program to Implement the Monoalphabetic Cypher

import java.io.*;
class monoalphabetic  {
	public static char normalChar[]
		= { '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' };

	public static char codedChar[]
		= { 'Q', 'W', 'E', 'R', 'T', 'Y', 'U', 'I', 'O',
			'P', 'A', 'S', 'D', 'F', 'G', 'H', 'J', 'K',
			'L', 'Z', 'X', 'C', 'V', 'B', 'N', 'M' };

	// Function which returns encrypted string
	public static String stringEncryption(String s)
	{
		// initializing an empty String
		String encryptedString = "";

		// comparing each character of the string and
		// encoding each character using the indices
		for (int i = 0; i < s.length(); i++) {
			for (int j = 0; j < 26; j++) {

				// comparing the character and
				// adding the corresponding char
				// to the encryptedString
				if (s.charAt(i) == normalChar[j])
				{
					encryptedString += codedChar[j];
					break;
				}

				// if there are any special characters
				// add them directly to the string
				if (s.charAt(i) < 'a' || s.charAt(i) > 'z')
				{
					encryptedString += s.charAt(i);
					break;
				}
			}
		}

		// return encryptedString
		return encryptedString;
	}

	// Function which returns descryptedString
	public static String stringDecryption(String s)
	{

		// Initializing the string
		String decryptedString = "";

		// Run the for loop for total string
		for (int i = 0; i < s.length(); i++)
		{
			for (int j = 0; j < 26; j++) {

				// compare each characters and decode them
				// using indices
				if (s.charAt(i) == codedChar[j])
				{
					decryptedString += normalChar[j];
					break;
				}

				// Add the special characters directly to
				// the String
				if (s.charAt(i) < 'A' || s.charAt(i) > 'Z')
				{
					decryptedString += s.charAt(i);
					break;
				}
			}
		}

		// return the decryptedString
		return decryptedString;
	}
	public static void main(String args[])
	{
		String str = "Priyush";
		// print plain text
		System.out.println("Plain text: " + str);
		String encryptedString = stringEncryption(str.toLowerCase());
		System.out.println("Encrypted message: " +	encryptedString );
		System.out.println("Decrypted message: "+ stringDecryption(encryptedString));

	}
}
```

⚫Output:

Advantages:

The increased security possible with variant multilateral systems is the major advantage.

Disadvantages.

The major disadvantage is that by substituting more than one character of ciphertext for each plaintext value, the length of messages and resulting transmission times are increased.

Conclusion: -

Thus, we have implemented Breaking the Mono-alphabetic Substitution Cipher using Frequency analysis method.