NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

LAB 02

LAB 02: To understand the process of Breaking the Mono-alphabetic Substitution Cipher using the Frequency analysis method

ROLL NO	52
NAME	Sarvesh Patil
CLASS	D15A
SUBJECT	Internet Security Lab
LO MAPPED	LO1: To apply the knowledge of symmetric cryptography to implement classical ciphers

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

AIM:
Write a program to understand the implementation of a product cipher using Substitution ciphers and Transposition Cipher.

INTRODUCTION:
Product Cipher:
In cryptography, a product cipher combines two or more transformations in a manner intending that the resulting cipher is more secure than the individual components to make it resistant to cryptanalysis. The product cipher combines a sequence of simple transformations such as substitution (S-box), permutation (P-box), and modular arithmetic. The concept of product ciphers is due to Claude Shannon, who presented the idea in his foundational paper, Communication Theory of Secrecy Systems.

For transformation involving a reasonable number of n message symbols, both of the foregoing cipher systems (the S-box and P-box) are by themselves wanting. Shannon suggested using a combination of S-box and P-box transformation—a product cipher. The combination could yield a cipher system more powerful than either one alone. This approach of alternatively applying substitution and permutation transformation has been used by IBM in the Lucifer cipher system and has become the standard for national data encryption standards such as the Data Encryption Standard and the Advanced Encryption Standard. A product cipher that uses only substitutions and permutations is called an SP network. Feistel ciphers are an important class of product ciphers.

Substitution Cipher:
Hiding some data is known as encryption. When plain text is encrypted it becomes unreadable and is known as ciphertext. In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by another character from the same set depending on a key. For example with a shift of 1, A would be replaced by B, B would become C, and so on. Note: Special case of Substitution cipher is known as Caesar cipher where the key is taken as 3.

Mathematical representation
The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25. Encryption of a letter by a shift n can be described mathematically as.

$E_n(x)=(x+n)mod\ 26$
(Encryption Phase with shift n)

$D_n(x)=(x-n)mod\ 26$
(Decryption Phase with shift n)

Examples:

1. Plain Text: I am studying Data Encryption
   Key: 4
   Output: M eq wxyhCmrk Hexe IrgvCtxmsr

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

2. Plain Text: ABCDEFGHIJKLMNOPQRSTUVWXYZ
   Key: 4
   Output: EFGHIJKLMNOPQRSTUVWXYZabcd

Input:
A String of both lower and upper case letters, called PlainText.
An Integer denoting the required key.

Procedure:
1. Create a list of all the characters.
2. Create a dictionary to store the substitution for all characters.
3. For each character, transform the given character as per the rule, depending on whether we're encrypting or decrypting the text.
4. Print the new string generated.

Transposition Cipher:
In cryptography, a transposition cipher is a method of encryption that scrambles the positions of characters (transposition) without changing the characters themselves. Transposition ciphers reorder units of plaintext (typically characters or groups of characters) according to a regular system to produce a ciphertext which is a permutation of the plaintext. They differ from substitution ciphers, which do not change the position of units of plaintext but instead change the units themselves. Despite the difference between transposition and substitution operations, they are often combined, as in historical ciphers like the ADFGVX cipher or complex high-quality encryption methods like the modern Advanced Encryption Standard (AES).
Plaintexts can be rearranged into ciphertext using a key, scrambling the order of characters like the shuffled pieces of a jigsaw puzzle. The resulting message is hard to decipher without the key because there are many ways the characters can be arranged.

For example, the plaintext "THIS IS WIKIPEDIA" could be encrypted to "TWDIP SIHII IKASE". To decipher the encrypted message without the key, an attacker could try to guess possible words and phrases like DIATHESIS, DISSIPATE, WIDTH, etc., but it would take them some time to reconstruct the plaintext because there are many combinations of letters and words. By contrast, someone with the key could reconstruct the message easily:

C I P H E R Key
1 4 5 3 2 6 Sequence (key letters in alphabetical order)
T H I S I S Plaintext
W I K I P E
D I A * * *

Ciphertext by column:
#1 TWD, #2 IP, #3 SI, #4 HII, #5 IKA, #6 SE
Ciphertext in groups of 5 for readability:
TWDIP SIHII IKASE
In practice, a message this short and with a predictable keyword would be broken almost immediately with cryptanalysis techniques. Transposition ciphers have several vulnerabilities (see

the section on "Detection and cryptanalysis" below), and small mistakes in the encipherment process can render the entire ciphertext meaningless.

However, given the right conditions - long messages (e.g., over 100–200 letters), unpredictable contents, unique keys per message, strong transposition methods, and so on - guessing the right words could be computationally impossible without further information. In their book on codebreaking historical ciphers, Elonka Dunin and Klaus Schmeh describe double columnar transposition (see below) as "one of the best manual ciphers known".

ALGORITHM:

STEP 1: Ask the user to enter plain text.
STEP 2: Ask a random number for a key to denote the required shift.
STEP 3: Call the function to substitute the given plain text.
STEP 4: Traverse the substituted text one character at a time.
STEP 5: Arrange the substituted text in transposition matrix column-wise with a number of rows equal to the random number taken as input from the user.
STEP 6: Traverse the transposition matrix row-wise to generate the final encrypted text.
STEP 7: Decrypt the encrypted text using the key to obtain the plain text back.

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

PROGRAM:

```
import java.time.Period;
import java.util.Arrays;
import java.util.Scanner;

public class ProductCipher {

   static void SubstitutionEncryption(String plainText, int key) {
      System.out.println("---Starting Substitution Encryption---");

      System.out.println("Your Plain Text : " + plainText);
      plainText = plainText.replace(" ", "");
      plainText = plainText.toLowerCase();
      char[] cypheredText = plainText.toCharArray();
      System.out.println("Plain Text after removing spaces :" + plainText);

      for (int i = 0; i < cypheredText.length; i++) {
         if ((int) cypheredText[i] + key >= 97 && (int) cypheredText[i] + key <= 122) {
            cypheredText[i] = (char) ((int) cypheredText[i] + key);
         }

         else if ((int) cypheredText[i] + key >= 123) {
            cypheredText[i] = (char) ((int) cypheredText[i] + key - 122 + 96);
         }

      }

      System.out.print("Ciphered Text After Substituion Cypher : ");
      System.out.println(cypheredText);
      System.out.println();
      TranspostionEncryption(cypheredText, key);
   }

   static void TranspostionEncryption(char[] cypheredText, int key) {
      char[][] TcypheredText = new char[cypheredText.length][cypheredText.length];
      int row = 0;
      int column = 0;
      System.out.println("---Starting Transpostion Encryption---");

      for (int i = 0; i < cypheredText.length; i++) {
         if (i == 0) {
            TcypheredText[row][column] = cypheredText[i];

            row++;
         }
```

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

```
        if (i != 0) {
            TcypheredText[row][column] = cypheredText[i];
            if (row + 1 >= key) {
                row = 0;
                column++;
            } else {
                row++;
            }
        }

    }

    System.out.println("");
    for (int i = 0; i < TcypheredText[column].length; i++) {
        for (int j = 0; j < TcypheredText[row].length; j++) {
            if ((int) TcypheredText[j][i] != 0) {
                System.out.print(TcypheredText[j][i] + " ");
            }
        }
        System.out.println();
    }
    String TraCypheredText = "";
    for (int i = 0; i < TcypheredText[column].length; i++) {
        for (int j = 0; j < TcypheredText[row].length; j++) {
            if ((int) TcypheredText[i][j] != 0) {
                TraCypheredText = TraCypheredText + TcypheredText[i][j];
            }

        }
    }
    System.out.println("Ciphered Text After Keyless Transpostion Cypher: " + TraCypheredText);
    System.out.println();

    TranspostionDecryption(TcypheredText, key, column, row);
}

static void TranspostionDecryption(char[][] TcypheredText, int key, int column, int row) {
    System.out.println("---Starting Transpostion Decryption---");
    String DeTra = "";

    for (int i = 0; i < TcypheredText[column].length; i++)

    {
        for (int j = 0; j < TcypheredText[row].length; j++) {
            if ((int) TcypheredText[j][i] != 0) {
                DeTra = DeTra + String.valueOf(TcypheredText[j][i]);
```

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

```
            }
        }
    }

    System.out.println("After Decryption of Transpositon Cypher, Cypher Text is : " + DeTra);
    System.out.println();

    SubstitutionDecryption(DeTra, key);
  }

  static void SubstitutionDecryption(String Detra, int key) {
    System.out.println("---Starting Subsitution Decryption---");
    char[] plainText = Detra.toCharArray();

    for (int i = 0; i < plainText.length; i++) {
      if ((int) plainText[i] - key >= 97 && (int) plainText[i] - key <= 122) {
        plainText[i] = (char) ((int) plainText[i] - key);
      }

      else if ((int) plainText[i] - key <= 98) {
        plainText[i] = (char) ((int) plainText[i] - key + 122 - 96);
      }

    }

    System.out.print("After Decryption of Substitution Cypher, Plane Text is : ");
    System.out.println(plainText);
    System.out.println();
  }

  public static void main(String[] args) {
    String plainText = "";
    int key = 0;
    Scanner sc = new Scanner(System.in);
    System.out.println("Enter text which has to be encrypted: ");
    plainText = sc.nextLine();
    System.out.println("Enter the key for encryption: ");
    key = sc.nextInt();
    System.out.println();
    SubstitutionEncryption(plainText, key);

  }
}
```

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

RESULTS:

1. ***Test Case 1:***
   Input Text: SarveshPatil
   Number: 4

```
❯ cd "/Users/sarveshpatil/Desktop/" && javac ProductCipher.java && java ProductCipher
Enter text which has to be encrypted:
SarveshPatil
Enter the key for encryption:
4

---Starting Substitution Encryption---
Your Plain Text : SarveshPatil
Plain Text after removing spaces :sarveshpatil
Ciphered Text After Substituion Cypher : wevziwltexmp

---Starting Transpostion Encryption---

w e v z
i w l t
e x m p




Ciphered Text After Keyless Transpostion Cypher: wieewxvlmztp

---Starting Transpostion Decryption---
After Decryption of Transpositon Cypher, Cypher Text is : wevziwltexmp

---Starting Subsitution Decryption---
After Decryption of Substitution Cypher, Plane Text is : sarveshpatil
```

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

2. ***Test Case 2:***
   Input Text: SarveshPatil
   Number: 0

```
❯ cd "/Users/sarveshpatil/Desktop/" && javac ProductCipher.java && java ProductCipher
Enter text which has to be encrypted:
SarveshPatil
Enter the key for encryption:
0

---Starting Substitution Encryption---
Your Plain Text : SarveshPatil
Plain Text after removing spaces :sarveshpatil
Ciphered Text After Substituion Cypher : sarveshpatil

---Starting Transpostion Encryption---

s a
r
v
e
s
h
p
a
t
i
l

Ciphered Text After Keyless Transpostion Cypher: srveshpatila

---Starting Transpostion Decryption---
After Decryption of Transpositon Cypher, Cypher Text is : sarveshpatil

---Starting Subsitution Decryption---
After Decryption of Substitution Cypher, Plane Text is : sarveshpatil
```

CONCLUSION:

We have successfully understood the implementation of a product cipher using Substitution ciphers and Transposition Cipher.