TCET

BE COMPUTER SCIENCE & ENGINEERING (CYBER SECURITY)

Choice Based Credit Grading System (CBCGS)

Under TCET Autonomy

# Experiment no. 2: Design & Implement Transposistion Cipher

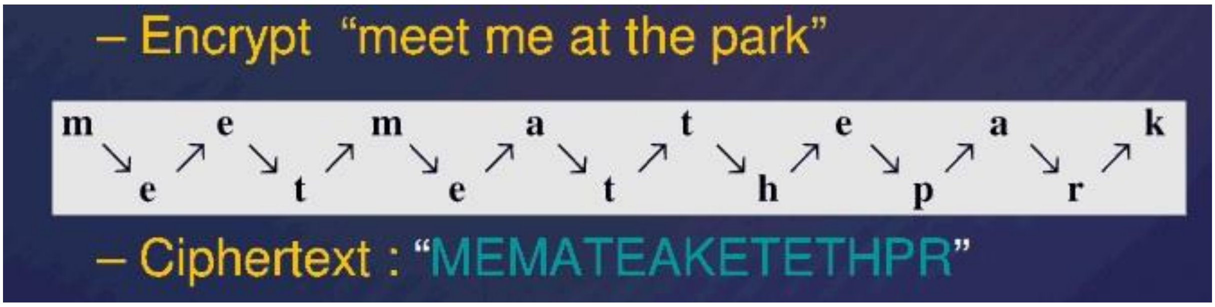
**Learning Objective**: Student should be able to design and implement Transposition Cipher.

**Tools:** C/C++/Java/Python or any computational software.

**Theory**: A Transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed (the plaintext is reordered). Mathematically a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt. Transposition Ciphers does not substitute one symbol for another, instead it changes thelocation of the symbols. A symbol in the first position of the plaintext may appear in the tenth position of the ciphertext. A symbol in the eight position in the plaintext may appear in the first position ofthe ciphertext. **A transposition cipher reorders (transposes) the symbols.** Simple transposition ciphers, which were used in the past, are keyless.

There are two methods for permutation of characters. In the first method, the text is writteninto a table column by column and then transmitted row by row. In the second method, thetext is written into a table row by row and then transmitted column by column.

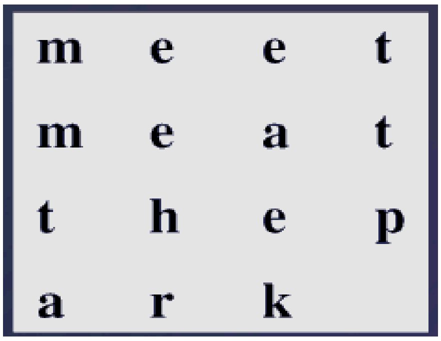
**Method I:**



– Encrypt "meet me at the park"

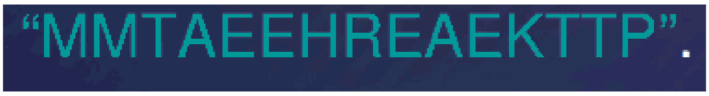
– Ciphertext : "MEMATEAKETETHPR"

**Method II:**



| | | | |
|---|---|---|---|
| m | e | e | t |
| m | e | a | t |
| t | h | e | p |
| a | r | k | |

**Cipher Text:**

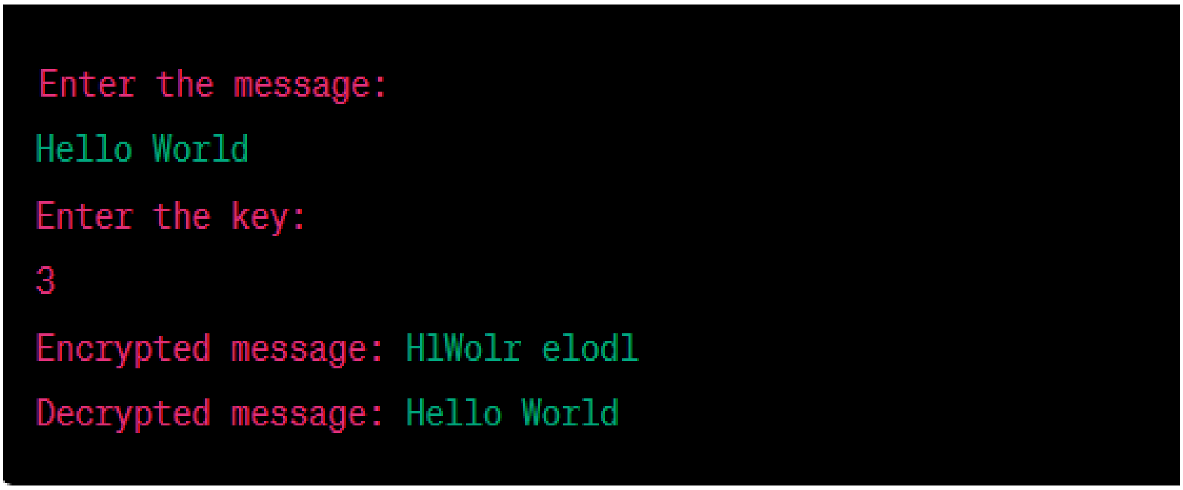


"MMTAEEHREAEKTTP".

## Source Code:

```
public class TranspositionCipher {
    public static String encrypt(String message, int key) {
        String result = "";
        int messageLength = message.length();
        int cipherSize = key * (int)Math.ceil((double)messageLength / key);
        char[][] cipher = new char[key][cipherSize];
        for (int i = 0; i < key; i++) {
            for (int j = 0; j < cipherSize; j++) {
                int position = i + j * key;
                if (position < messageLength) {
                    cipher[i][j] = message.charAt(position);
                } else {
                    cipher[i][j] = ' ';
                }
            }
        }
        for (int i = 0; i < key; i++) {
            for (int j = 0; j < cipherSize; j++) {
                result += cipher[j][i];
            }
        }
        return result;
    }
    public static String decrypt(String message, int key) {
        String result = "";
        int messageLength = message.length();
    int cipherSize = key * (int)Math.ceil((double)messageLength / key);
    char[][] cipher = new char[key][cipherSize];
    for (int i = 0; i < key; i++) {
      for (int j = 0; j < cipherSize; j++) {
        int position = i + j * key;
        if (position < messageLength) {
          cipher[j][i] = message.charAt(position);
        } else {
          cipher[j][i] = ' ';
        }
      }
    }
    for (int i = 0; i < cipherSize; i++) {
      for (int j = 0; j < key; j++) {
        result += cipher[i][j];
      }
    }
    return result.trim();
  }
public static void main(String[] args) {
    String message = "This is a secret message";
    int key = 4;
    String encryptedMessage = encrypt(message, key);
    String decryptedMessage = decrypt(encryptedMessage, key);
    System.out.println("Original Message: " + message);
    System.out.println("Encrypted Message: " + encryptedMessage);
    System.out.println("Decrypted Message: " + decryptedMessage);
  }}
```

## Output:



```
Enter the message:
Hello World
Enter the key:
3
Encrypted message: HlWolr elodl
Decrypted message: Hello World
```

## Applications:

- **Historical Military Communication:** Transposition ciphers were historically used in military communication to encode sensitive information. During wartime, military units would employ transposition ciphers to ensure that intercepted messages were indecipherable to the enemy.
- **Privacy in Digital Communication:** Despite being relatively simple, transposition ciphers can still provide a level of privacy in digital communication. They can be used for encrypting emails, messages, or any other form of digital communication, especially when combined with other cryptographic techniques.

## Result & Discussion:

The experiment implementing a transposition cipher in Java, the algorithm successfully encrypted and decrypted messages based on the provided key. The output demonstrated the rearrangement of characters according to the transposition key, showcasing the cipher's functionality in encoding and decoding messages.

**Learning Outcomes:** The student should have the ability to design & implement Transposition Cipher

**LO1:** To describe & understand about Transposition cipher techniques

**LO2:** To implement Transposition cipher techniques

**Course Outcomes:** Upon completion of the course students will be able to understand & implement Substitution Cipher.

**Conclusion:** In conclusion, the implemented transposition cipher experiment showcased the algorithm's functionality through encryption and decryption functions, utilizing row-column rearrangement based on a user-provided key. With a time complexity proportional to the length of the message and key, the cipher demonstrated simplicity and efficiency in encoding and decoding plaintext.

**NAME: Aryan Tiwari**

**CLASS: SE – CSE**

**ROLL NO: 57**

**For Faculty Use**

| Correction Parameters | Formative Assessment [40%] | Timely completion of Practical<br>[ 40%] | Attendance / Learning Attitude [20%] | |
|---|---|---|---|---|
| Marks Obtained | | | | |