SUB: Information Security

AY 2023-24 (Semester-V)

Name: Divyesh Khunt Sapid:60009210116 Batch:D12

Experiment No: 4

Aim: To Implement Encryption and Decryption using Columnar Transposition Cipher.

Theory:

1. Transposition Cipher
2. Columnar Transposition Cipher/ Row Column Transposition Cipher.

Example:
Encryption and Decryption

1) **Plaintext : "Attack Postponed until two am"**
   Keyword: 4312567
   Ciphertext:

SUB: Information Security

```python
import math
key = '4312567'
def encryptMessage(msg):
    cipher = ""
    msg_len = len(msg)
    key_lst = sorted(list(key))
    col = len(key)
    row = int(math.ceil(msg_len / col))
    matrix = [msg[i:i + col] for i in range(0, len(msg), col)]

    for _ in range(col):
        curr_idx = key.index(key_lst[_])
        k_indx = 0
        for row_idx in range(row):
            if (row_idx * col + curr_idx) < msg_len:
                cipher += matrix[row_idx][curr_idx]
            k_indx += 1

    return cipher
```

```python
[26] def decryptMessage(cipher):
        msg = ""
        k_indx = 0
        msg_indx = 0
        msg_len = len(cipher)
        msg_lst = list(cipher)
        col = len(key)
        row = int(math.ceil(msg_len / col))
        key_lst = sorted(list(key))
        dec_cipher = []
        for _ in range(row):
            dec_cipher += [['_'] * col]
        for _ in range(col):
            curr_idx = key.index(key_lst[k_indx])
            for j in range(row):
                if (j * col + curr_idx) < msg_len:
                    dec_cipher[j][curr_idx] = msg_lst[msg_indx]
                    msg_indx += 1
            k_indx += 1
            msg = ''.join(''.join(row) for row in dec_cipher)
        return msg.replace('_', '')
```

SUB: Information Security

```
msg = "Attack Postponed until two am"
print("Plain text:",msg)
cipher = encryptMessage(msg)
print("Encrypted Message: {}".format(cipher))
decrypted_msg = decryptMessage(cipher)
print("Decrypted Message: {}".format(decrypted_msg))
```

```
Plain text: Attack Postponed until two am
Encrypted Message: ts tatuwtod APelmcpnokot  nia
Decrypted Message: Attack Postponed until two am
```

Conclusion:
Thus transformation Cipher was implemented successfully.