INSTITUTE OF COMPUTER TECHNOLOGY

B-TECH COMPUTER SCIENCE ENGINEERING 2025-26

SUBJECT:-CRYPTOGRAPHY

NAME: Rahul Prajapati

ENRLL. NO: 23162171020

BRANCH: CYBER SECURITY

BATCH: 52

PRACTICAL_6

Aim: To understand the concept of Transposition Ciphers by implementing the Columnar Transposition Cipher for both encryption and decryption, and to analyze how transposition differs from substitution in terms of security and attack methods.

CODE:

```python
def encrypt(plain_text, keyword):
    columns = [""] * len(keyword)
    for i, char in enumerate(plain_text):
        columns[i % len(keyword)] += char
    sorted_keyword = sorted((char, i) for i, char in enumerate(keyword))
    cipher_text = "".join(columns[i] for char, i in sorted_keyword)
    return cipher_text


def decrypt(cipher_text, keyword):
    num_full_rows = len(cipher_text) // len(keyword)
    num_short_cols = len(cipher_text) % len(keyword)

    col_lengths = [
        num_full_rows + (1 if i < num_short_cols else 0) for i in range(len(keyword))
    ]

    sorted_keyword = sorted((char, i) for i, char in enumerate(keyword))

    columns = [""] * len(keyword)

    index = 0
    for char, i in sorted_keyword:
        columns[i] = cipher_text[index : index + col_lengths[i]]
        index += col_lengths[i]

    plain_text = ""
    for row in range(num_full_rows + (1 if num_short_cols > 0 else 0)):
        for col in range(len(keyword)):
            if row < len(columns[col]):
                plain_text += columns[col][row]

    return plain_text
```

```python
if __name__ == "__main__":
    text = "HELLOTRANSPOSITIONCIPHER"
    keyword = "KEYWORD"

    print(f"Keyword: {keyword}")
    encrypted = encrypt(text, keyword)
    print("Encrypted:", encrypted)

    decrypted = decrypt(encrypted, keyword)
    print("Decrypted:", decrypted)
    keywords = ["KEY", "WORD", "LONGERKEY"]
    for kw in keywords:
        print(f"\nKeyword: {kw}")
        encrypted = encrypt(text, kw)
        print("Encrypted:", encrypted)

        decrypted = decrypt(encrypted, kw)
        print("Decrypted:", decrypted)
    text_with_padding = "HELLOTRANSPOSITIONCIPHE"
    keyword = "PADDING"
    print(f"\nKeyword: {keyword} with padding")
    encrypted = encrypt(text_with_padding, keyword)
    print("Encrypted:", encrypted)

    decrypted = decrypt(encrypted, keyword)
    print("Decrypted:", decrypted)
```

OUTPUT:

```
[Running] python -u "c:\Users\Hp\OneDrive\Desktop\SEM_05\Cryptography\Practicals_source_code\practical6_1.py"
Keyword: KEYWORD
Encrypted: RIPENIEHATHOOCTSILPNLSOR
Decrypted: HELLOTRANSPOSITIONCIPHER

Keyword: KEY
Encrypted: EOAPIOIEHLRSSICHLTNOTNPR
Decrypted: HELLOTRANSPOSITIONCIPHER

Keyword: WORD
Encrypted: LAOIIRETSINHLRPTCEHONSOP
Decrypted: HELLOTRANSPOSITIONCIPHER

Keyword: LONGERKEY
Encrypted: OIEAOLSHRIHSCLOPEPITTRNN
Decrypted: HELLOTRANSPOSITIONCIPHER

Keyword: PADDING with padding
Encrypted: ENIELSOLPNRIPOOCTSIHATH
Decrypted: HELLOTRANSPOSITIONCIPHE
```