

ASSIGNMENT-4

Implement the Hill Cipher encryption algorithm using Python and simulate how it could be used to secure user input (like messages from a contact form on your landing page).

```
import numpy as np

def preprocess_message(message, block_size):
    message = message.replace(" ", "").upper()
    while len(message) % block_size != 0:
        message += "x"
    return message

def char_to_num(c):
    return ord(c) - ord('A')

def num_to_char(n):
    return chr((n % 26) + ord('A'))

def encrypt(message, key_matrix):
    block_size = key_matrix.shape[0]
    message = preprocess_message(message, block_size)
    ciphertext = ""
    for i in range(0, len(message), block_size):
        block = message[i:i + block_size]
        vector = np.array([char_to_num(c) for c in block])
        encrypted_vector = np.dot(key_matrix, vector)
        ciphertext += ''.join(num_to_char(num) for num in encrypted_vector)
    return ciphertext

if __name__ == "__main__":
    msg = input("Enter the message to encrypt: ")
    size = int(input("Enter key matrix size (2 or 3): "))
    print(f"Enter the {size}x{size} key matrix row by row (space-separated numbers):")
    key_matrix = []
    for i in range(size):
        row = list(map(int, input(f"Row {i+1}: ").split()))
        if len(row) != size:
            raise ValueError("Each row must have the same number of elements as the matrix size.")
        key_matrix.append(row)

    key_matrix = np.array(key_matrix)
    encrypted = encrypt(msg, key_matrix)
    print(f"\nPlaintext: {msg}")
    print(f"Ciphertext: {encrypted}")
```

OUTPUT:

```
PS C:\Users\naddu\Desktop\CGNS> & "C:/Program Files/Python311/python3.11t.exe" c:/Users/naddu/Desktop/CGNS/HillCypher.py
Enter the message to encrypt: HELLO WORLD
Enter key matrix size (2 or 3): 2
Enter the 2x2 key matrix row by row (space-separated numbers):
Row 1: 3 3
Row 2: 2 5

Plaintext: HELLO WORLD
Ciphertext: HEOZEIPXQL
```

```
PS C:\Users\naddu\Desktop\CGNS> & "C:/Program Files/Python311/python3.11t.exe" c:/Users/naddu/Desktop/CGNS/HillCypher.py
Enter the message to encrypt: Cryptography and Computer Networks
Enter key matrix size (2 or 3): 2
Enter the 2x2 key matrix row by row (space-separated numbers):
Row 1: 3 3
Row 2: 2 5

Plaintext: Cryptography and Computer Networks
Ciphertext: FLNIVERTTXPENNPQNBARGMVRZEKDGTV
```