Syed Shaheer Ali Zaidi B20102168

Vernam Cipher

Code :

```python
alphabet = ['A','B','C','D','E','F','G','H','I','J','K','L','M','N','O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']

def cipher(M, K, c):
    C=[]
    for i in range (len(M)):
        if (c == 1):
            xor = M[i] + K[i%len(key)]
            C.append(alphabet[xor%26])
        if (c == 2):
            xor = M[i] - K[i%len(key)]
            C.append(alphabet[xor%26])
    print (C)

message = str(input("Input message in uppercase : "))
key = str(input("Input Key in uppercase : "))
c = int(input("1. Encrypt\n2. Decrypt\n"))
temp = []
M=[]
K=[]

for i in range(len(message)):
        if message[i].isalpha():
            temp.append(ord(message[i]))
            M.append(temp[-1] - ord('A'))

for i in range(len(key)):
        if key[i].isalpha():
            temp.append(ord(key[i]))
            K.append(temp[-1] - ord('A'))

cipher (M, K, c)
```

Output:

```
Input message in uppercase : HELLOWORLD
Input Key in uppercase : TEST
1. Encrypt
2. Decrypt
1
['A', 'I', 'D', 'E', 'H', 'A', 'G', 'K', 'E', 'H']
```

```
Input message in uppercase : AIDEHAGKEH
Input Key in uppercase : TEST
1. Encrypt
2. Decrypt
2
['H', 'E', 'L', 'L', 'O', 'W', 'O', 'R', 'L', 'D']
```