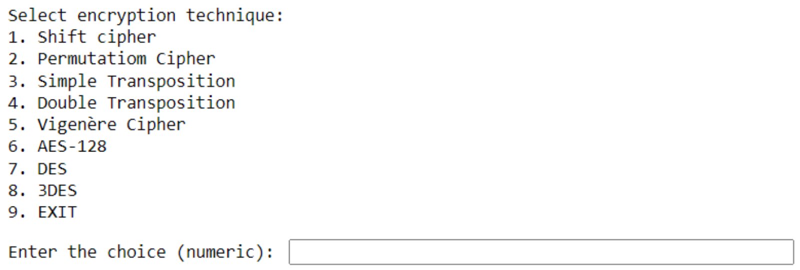
CS 458 – Coding Assignment II

A20551908

VADLAMUDI MANOGNA

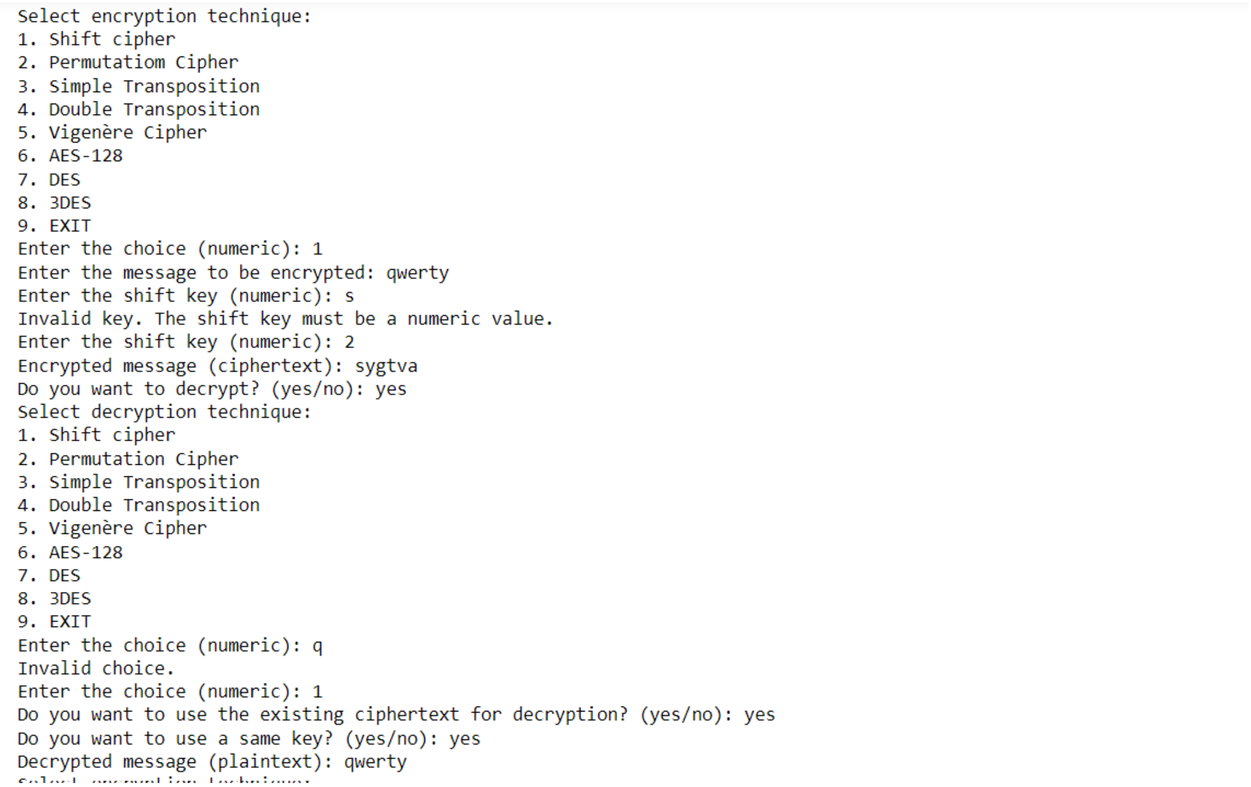
The program initially displays the following options on execution:



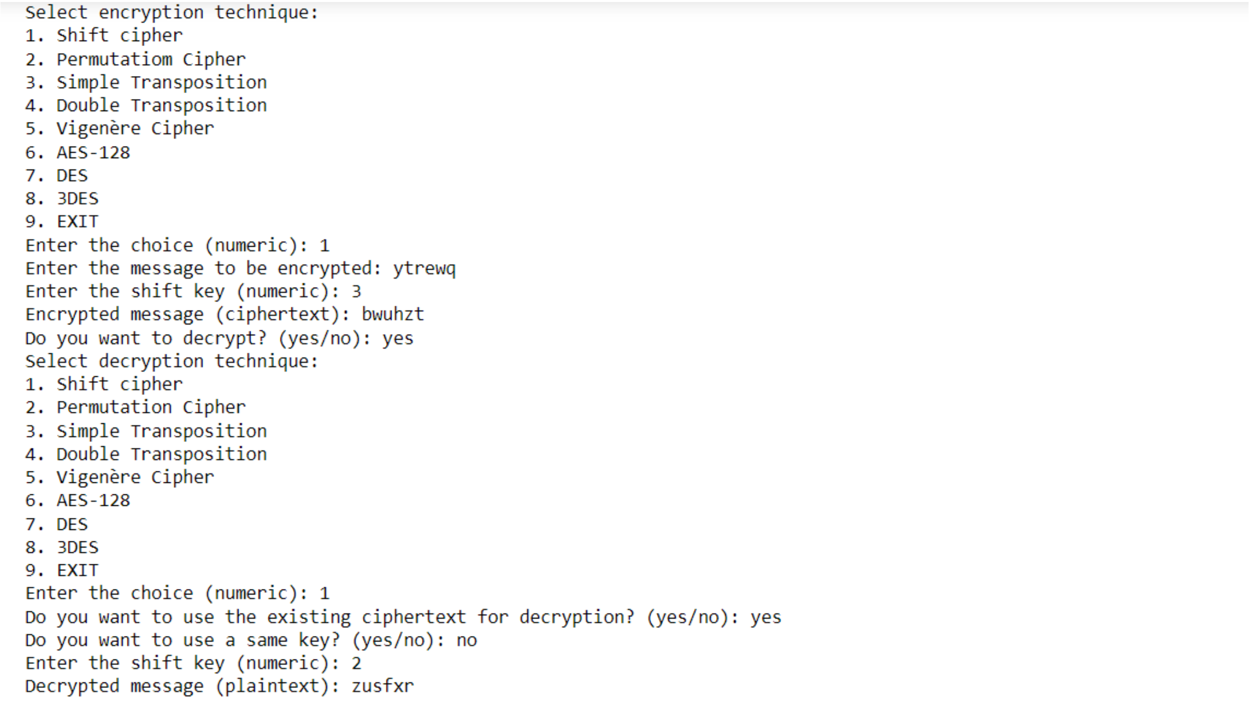
```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT

Enter the choice (numeric):
```

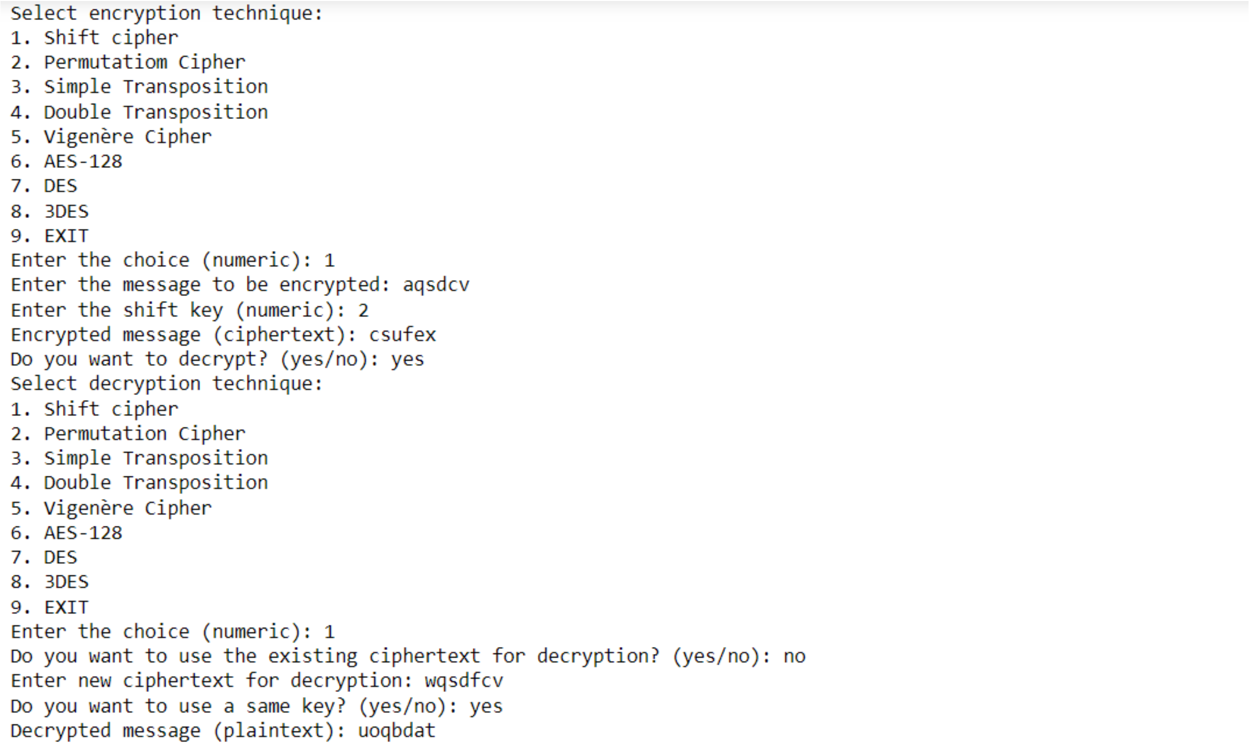
For 1(choice:1 – Shift cipher)



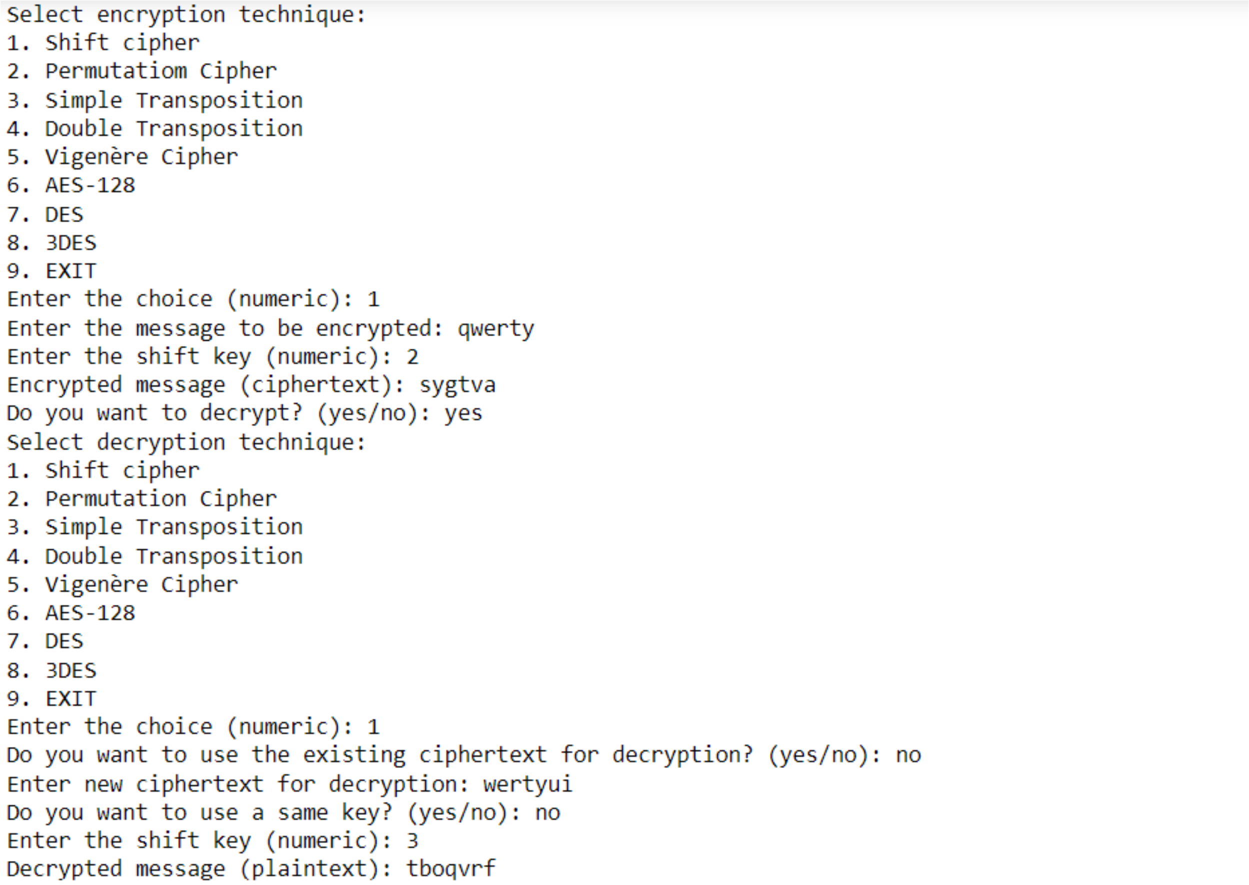
```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 1
Enter the message to be encrypted: qwerty
Enter the shift key (numeric): s
Invalid key. The shift key must be a numeric value.
Enter the shift key (numeric): 2
Encrypted message (ciphertext): sygtva
Do you want to decrypt? (yes/no): yes
Select decryption technique:
1. Shift cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): q
Invalid choice.
Enter the choice (numeric): 1
Do you want to use the existing ciphertext for decryption? (yes/no): yes
Do you want to use a same key? (yes/no): yes
Decrypted message (plaintext): qwerty
```



```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 1
Enter the message to be encrypted: ytrewq
Enter the shift key (numeric): 3
Encrypted message (ciphertext): bwuhzt
Do you want to decrypt? (yes/no): yes
Select decryption technique:
1. Shift cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 1
Do you want to use the existing ciphertext for decryption? (yes/no): yes
Do you want to use a same key? (yes/no): no
Enter the shift key (numeric): 2
Decrypted message (plaintext): zusfxr
```

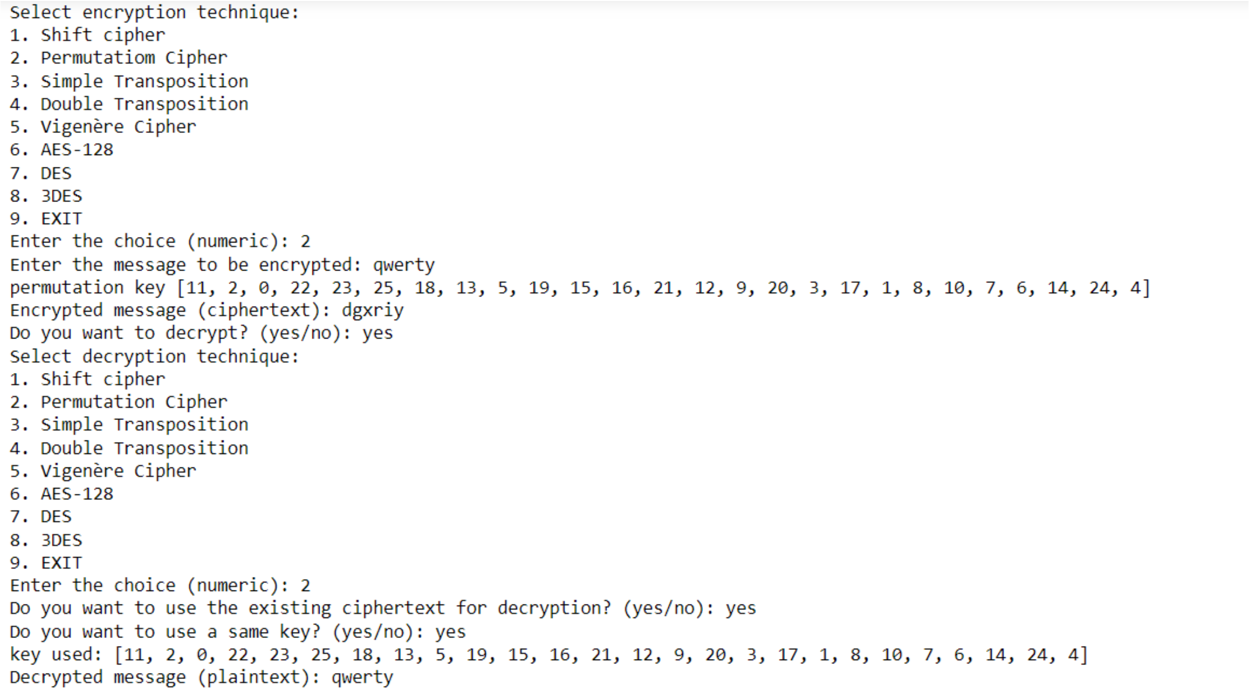


```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 1
Enter the message to be encrypted: aqsdcv
Enter the shift key (numeric): 2
Encrypted message (ciphertext): csufex
Do you want to decrypt? (yes/no): yes
Select decryption technique:
1. Shift cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 1
Do you want to use the existing ciphertext for decryption? (yes/no): no
Enter new ciphertext for decryption: wqsdfcv
Do you want to use a same key? (yes/no): yes
Decrypted message (plaintext): uoqbdat
```

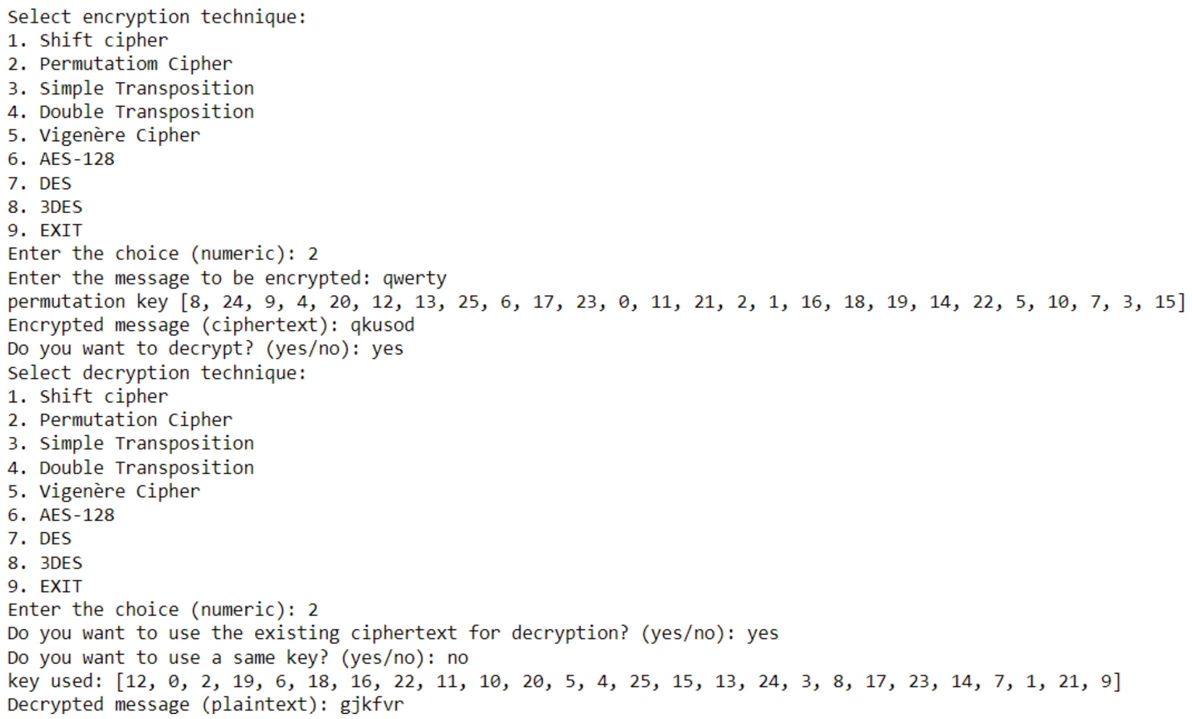


```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 1
Enter the message to be encrypted: qwerty
Enter the shift key (numeric): 2
Encrypted message (ciphertext): sygtva
Do you want to decrypt? (yes/no): yes
Select decryption technique:
1. Shift cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 1
Do you want to use the existing ciphertext for decryption? (yes/no): no
Enter new ciphertext for decryption: wertyui
Do you want to use a same key? (yes/no): no
Enter the shift key (numeric): 3
Decrypted message (plaintext): tboqvrf
```

For 2(choice: 2 – Permutation cipher)

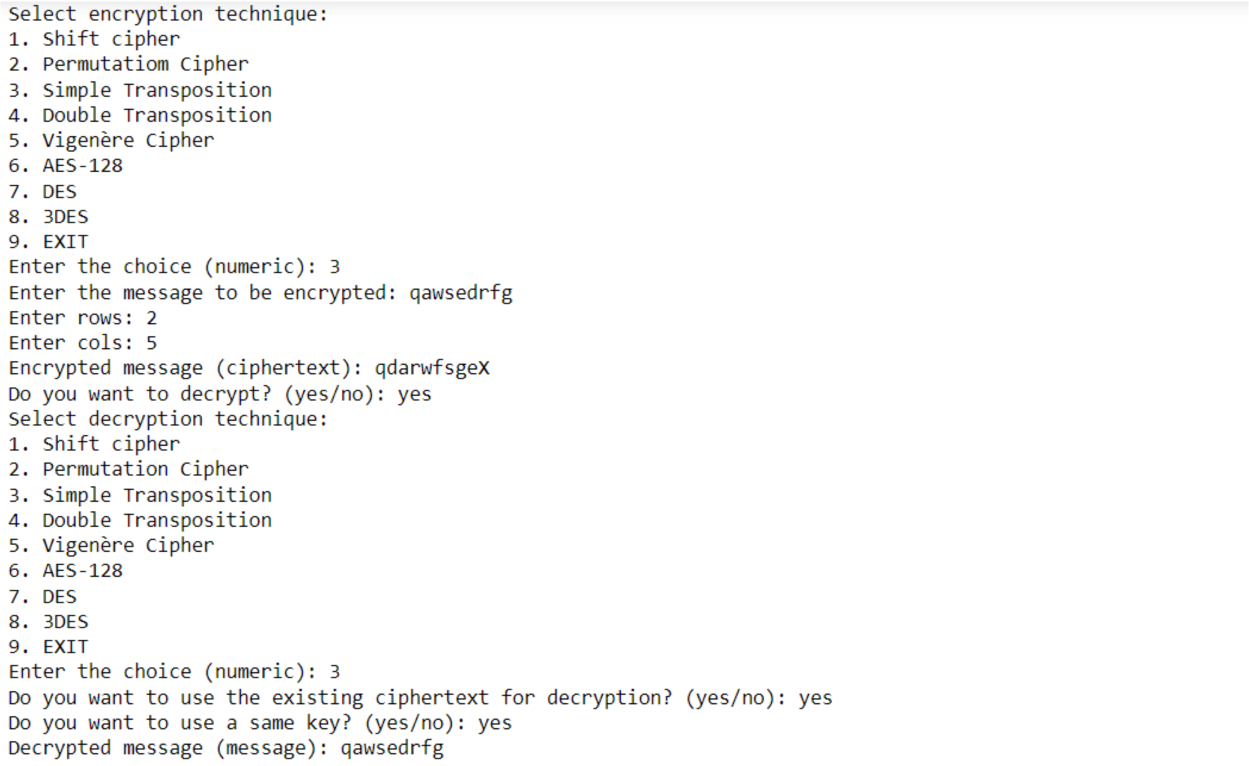


```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 2
Enter the message to be encrypted: qwerty
permutation key [11, 2, 0, 22, 23, 25, 18, 13, 5, 19, 15, 16, 21, 12, 9, 20, 3, 17, 1, 8, 10, 7, 6, 14, 24, 4]
Encrypted message (ciphertext): dgxriy
Do you want to decrypt? (yes/no): yes
Select decryption technique:
1. Shift cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 2
Do you want to use the existing ciphertext for decryption? (yes/no): yes
Do you want to use a same key? (yes/no): yes
key used: [11, 2, 0, 22, 23, 25, 18, 13, 5, 19, 15, 16, 21, 12, 9, 20, 3, 17, 1, 8, 10, 7, 6, 14, 24, 4]
Decrypted message (plaintext): qwerty
```



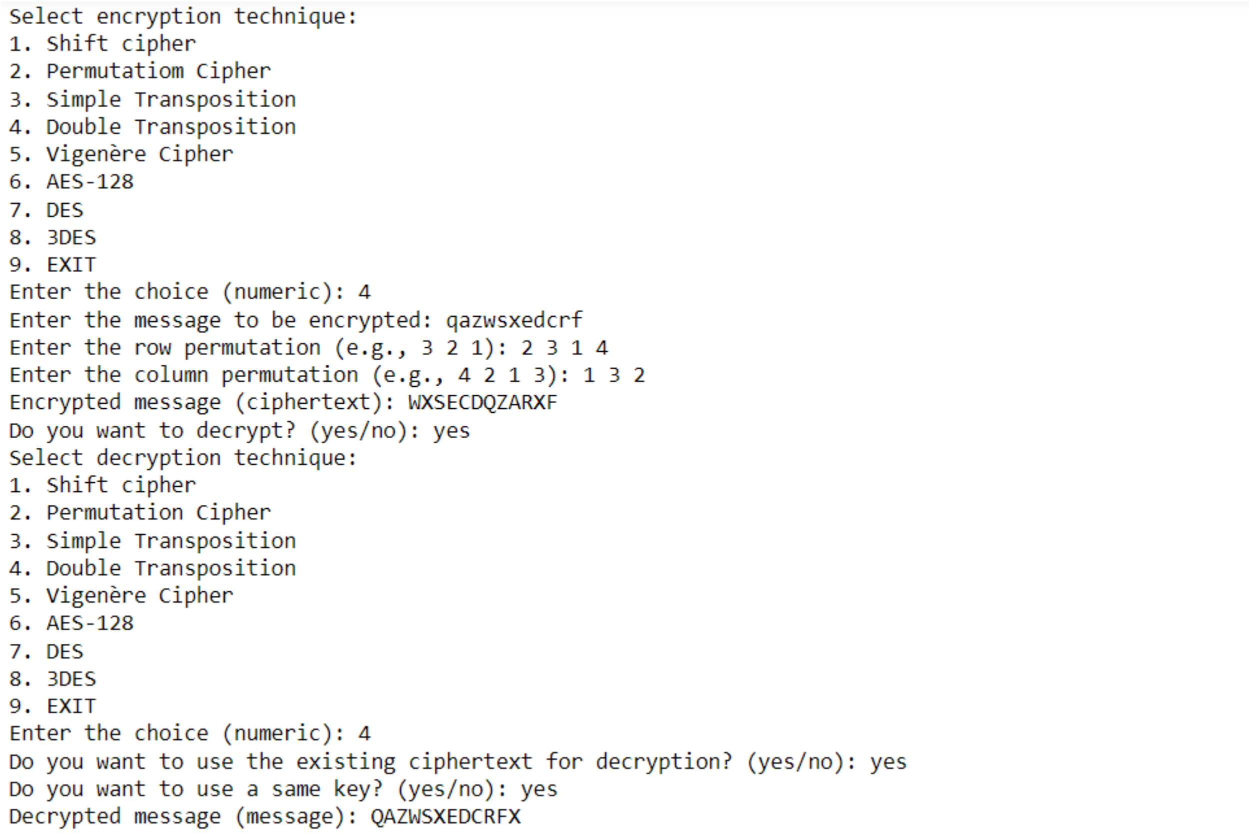
```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 2
Enter the message to be encrypted: qwerty
permutation key [8, 24, 9, 4, 20, 12, 13, 25, 6, 17, 23, 0, 11, 21, 2, 1, 16, 18, 19, 14, 22, 5, 10, 7, 3, 15]
Encrypted message (ciphertext): qkusod
Do you want to decrypt? (yes/no): yes
Select decryption technique:
1. Shift cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 2
Do you want to use the existing ciphertext for decryption? (yes/no): yes
Do you want to use a same key? (yes/no): no
key used: [12, 0, 2, 19, 6, 18, 16, 22, 11, 10, 20, 5, 4, 25, 15, 13, 24, 3, 8, 17, 23, 14, 7, 1, 21, 9]
Decrypted message (plaintext): gjkfvr
```

For (choice: 3 – Simple Transposition)



```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 3
Enter the message to be encrypted: qawsedrfg
Enter rows: 2
Enter cols: 5
Encrypted message (ciphertext): qdarwfsgeX
Do you want to decrypt? (yes/no): yes
Select decryption technique:
1. Shift cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 3
Do you want to use the existing ciphertext for decryption? (yes/no): yes
Do you want to use a same key? (yes/no): yes
Decrypted message (message): qawsedrfg
```

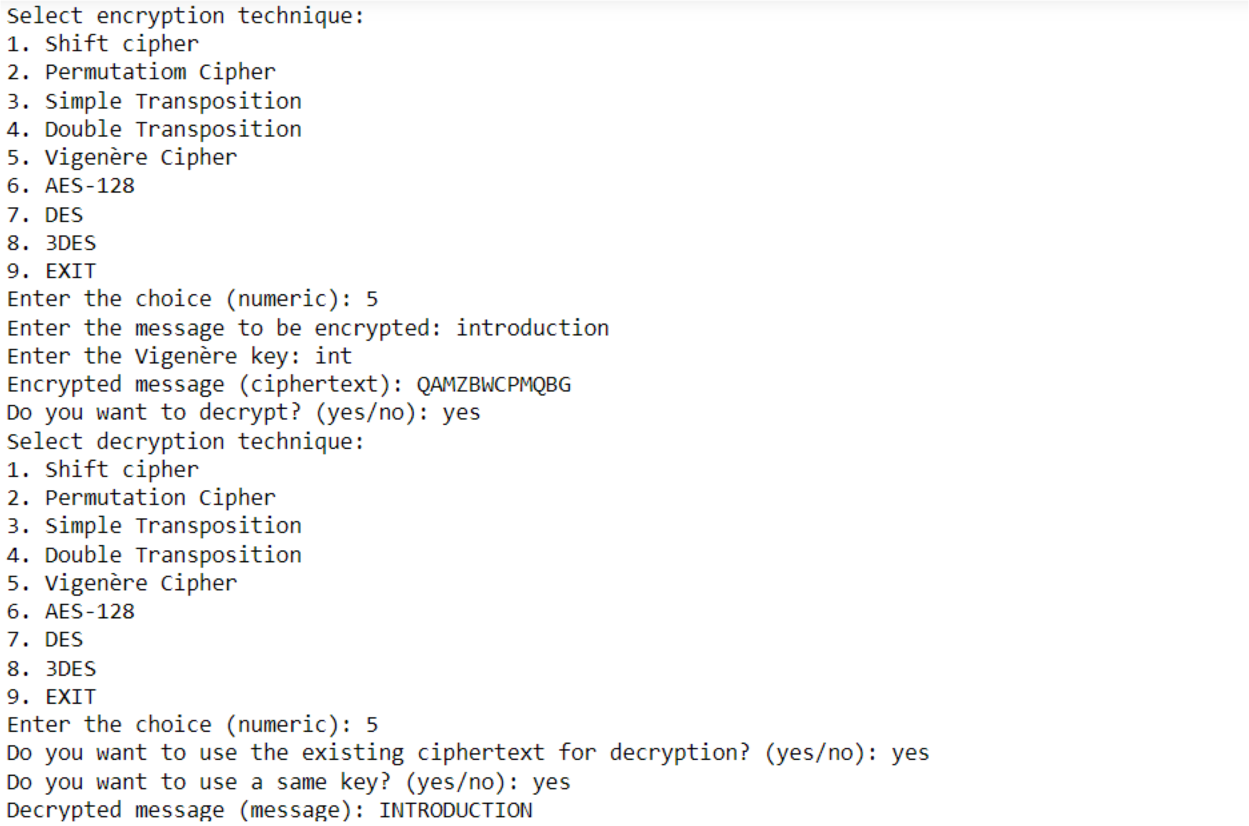
For (choice: 4 – Double Transposition)



```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 4
Enter the message to be encrypted: qazwsxedcrf
Enter the row permutation (e.g., 3 2 1): 2 3 1 4
Enter the column permutation (e.g., 4 2 1 3): 1 3 2
Encrypted message (ciphertext): WXSECDQZARXF
Do you want to decrypt? (yes/no): yes
Select decryption technique:
1. Shift cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 4
Do you want to use the existing ciphertext for decryption? (yes/no): yes
Do you want to use a same key? (yes/no): yes
Decrypted message (message): QAZWSXEDCRFX
```

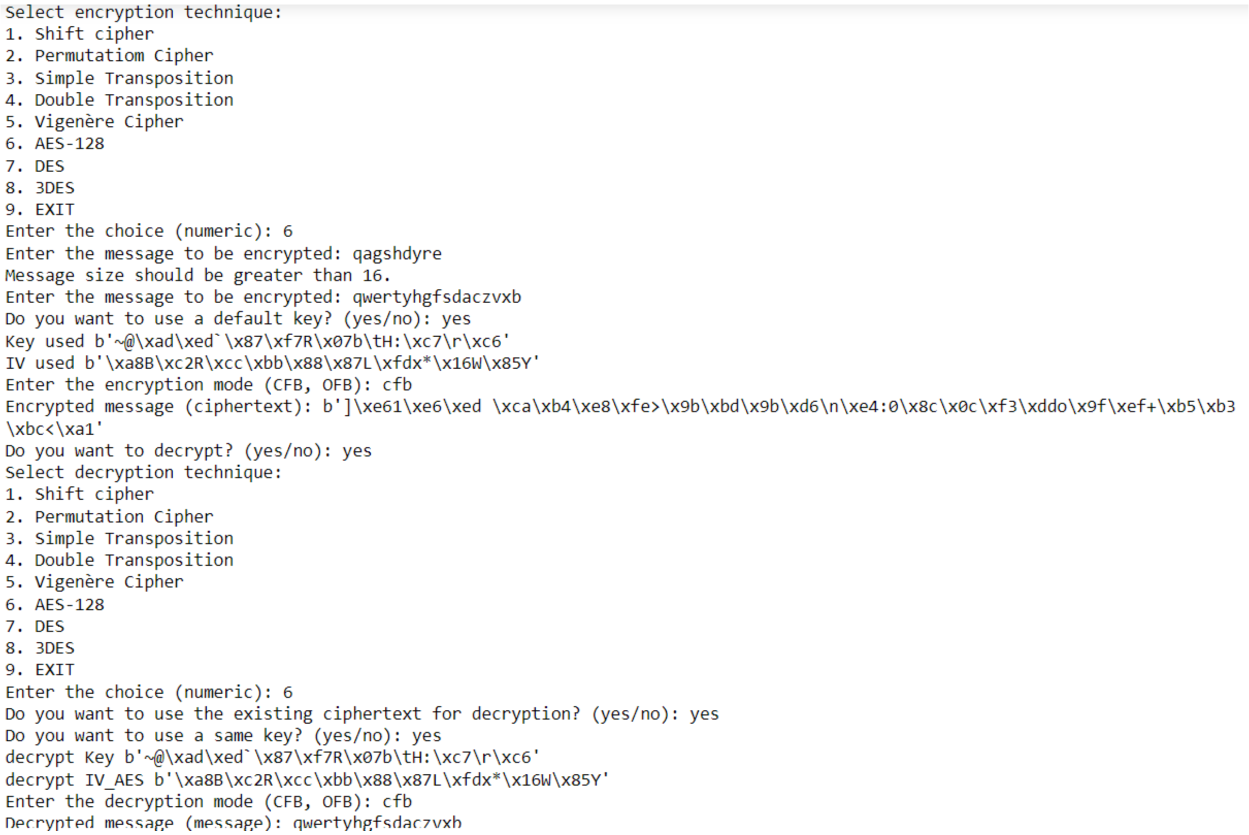
Here x in decrypted message at the end is an extra character. As our input has only 11 characters but the matrix is 4x3 which is 12.

For (choice: 5 – Vigenère Cipher)



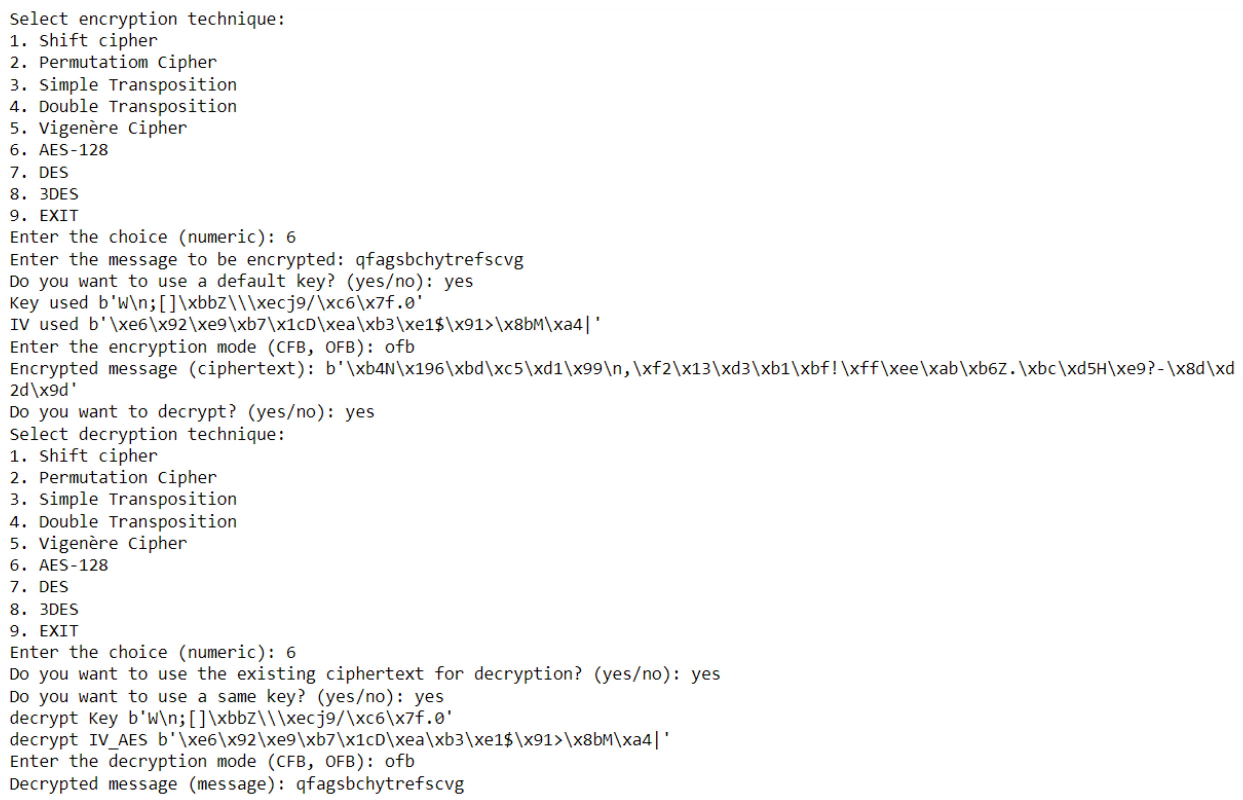
```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 5
Enter the message to be encrypted: introduction
Enter the Vigenère key: int
Encrypted message (ciphertext): QAMZBWCPMQBG
Do you want to decrypt? (yes/no): yes
Select decryption technique:
1. Shift cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 5
Do you want to use the existing ciphertext for decryption? (yes/no): yes
Do you want to use a same key? (yes/no): yes
Decrypted message (message): INTRODUCTION
```

For (choice: 6 – AES-128)
Case1: CFB



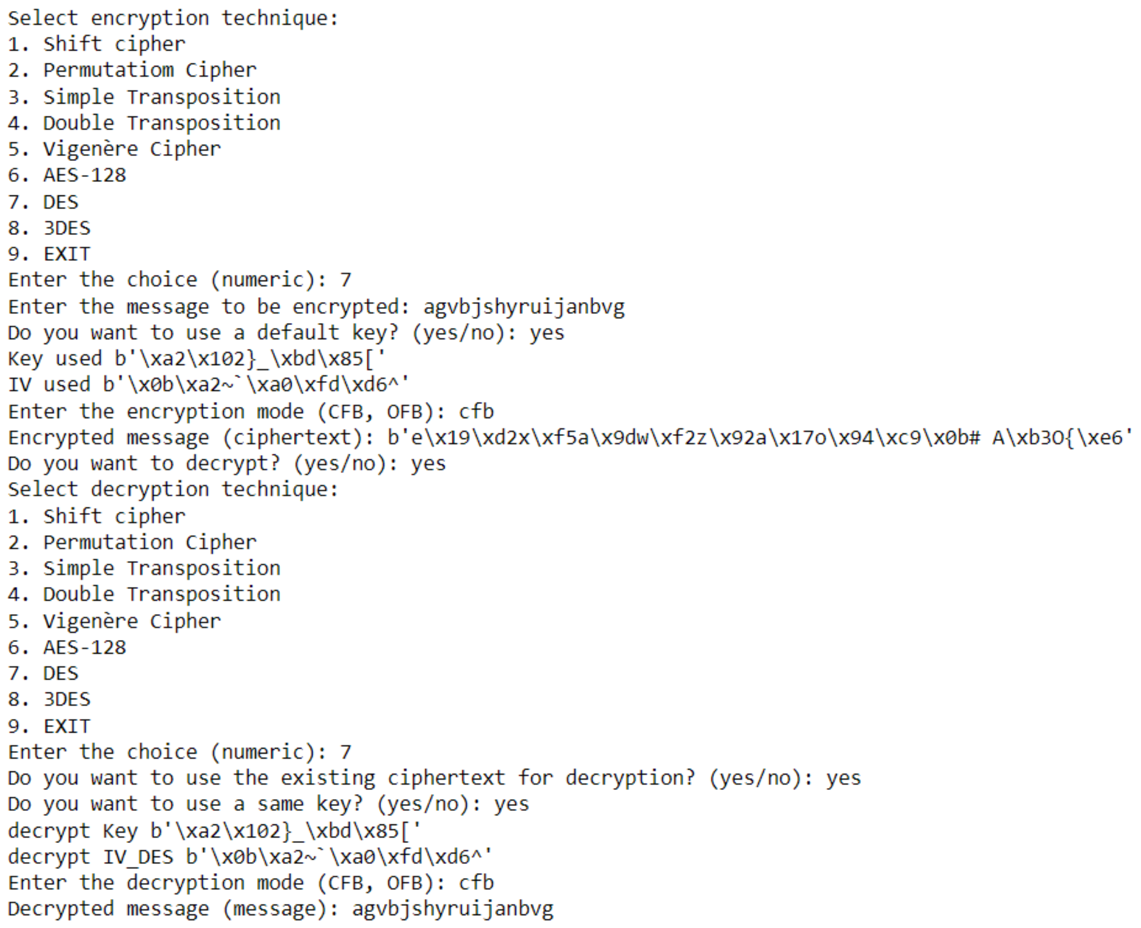
```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 6
Enter the message to be encrypted: qagshdyre
Message size should be greater than 16.
Enter the message to be encrypted: qwertyhgfsdaczvxb
Do you want to use a default key? (yes/no): yes
Key used b'~@\xad\xed`\x87\xf7R\x07b\tH:\xc7\r\xc6'
IV used b'\xa8B\xc2R\xcc\xbb\x88\x87L\xfdx*\x16W\x85Y'
Enter the encryption mode (CFB, OFB): cfb
Encrypted message (ciphertext): b']\xe61\xe6\xed \xca\xb4\xe8\xfe>\x9b\xbd\x9b\xd6\n\xe4:0\x8c\x0c\xf3\xddo\x9f\xef+\xb5\xb3
\xbc<\xa1'
Do you want to decrypt? (yes/no): yes
Select decryption technique:
1. Shift cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 6
Do you want to use the existing ciphertext for decryption? (yes/no): yes
Do you want to use a same key? (yes/no): yes
decrypt Key b'~@\xad\xed`\x87\xf7R\x07b\tH:\xc7\r\xc6'
decrypt IV_AES b'\xa8B\xc2R\xcc\xbb\x88\x87L\xfdx*\x16W\x85Y'
Enter the decryption mode (CFB, OFB): cfb
Decrypted message (message): qwertyhgfsdaczvxb
```

Case2: OFB



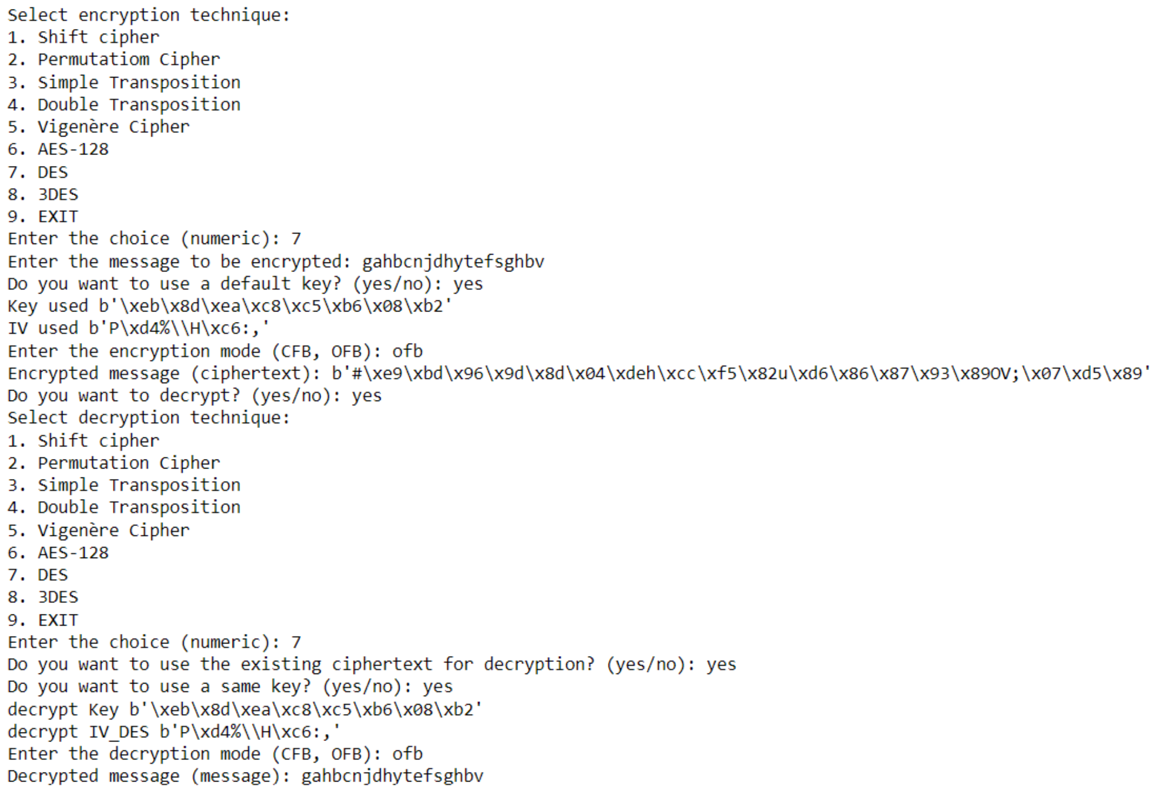
```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 6
Enter the message to be encrypted: qfagsbchytrefscvg
Do you want to use a default key? (yes/no): yes
Key used b'W\n;[]\xbbZ\\\xecj9/\xc6\x7f.0'
IV used b'\xe6\x92\xe9\xb7\x1cD\xea\xb3\xe1$\x91>\x8bM\xa4|'
Enter the encryption mode (CFB, OFB): ofb
Encrypted message (ciphertext): b'\xb4N\x196\xbd\xc5\xd1\x99\n,\xf2\x13\xd3\xb1\xbf!\xff\xee\xab\xb6Z.\xbc\xd5H\xe9?-\x8d\xd
2d\x9d'
Do you want to decrypt? (yes/no): yes
Select decryption technique:
1. Shift cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 6
Do you want to use the existing ciphertext for decryption? (yes/no): yes
Do you want to use a same key? (yes/no): yes
decrypt Key b'W\n;[]\xbbZ\\\xecj9/\xc6\x7f.0'
decrypt IV_AES b'\xe6\x92\xe9\xb7\x1cD\xea\xb3\xe1$\x91>\x8bM\xa4|'
Enter the decryption mode (CFB, OFB): ofb
Decrypted message (message): qfagsbchytrefscvg
```

For (choice: 7 – DES)
Case1: CFB



```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 7
Enter the message to be encrypted: agvbjshyruijanbvg
Do you want to use a default key? (yes/no): yes
Key used b'\xa2\x102}_\xbd\x85['
IV used b'\x0b\xa2~`\xa0\xfd\xd6^'
Enter the encryption mode (CFB, OFB): cfb
Encrypted message (ciphertext): b'e\x19\xd2x\xf5a\x9dw\xf2z\x92a\x17o\x94\xc9\x0b# A\xb3O{\xe6'
Do you want to decrypt? (yes/no): yes
Select decryption technique:
1. Shift cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 7
Do you want to use the existing ciphertext for decryption? (yes/no): yes
Do you want to use a same key? (yes/no): yes
decrypt Key b'\xa2\x102}_\xbd\x85['
decrypt IV_DES b'\x0b\xa2~`\xa0\xfd\xd6^'
Enter the decryption mode (CFB, OFB): cfb
Decrypted message (message): agvbjshyruijanbvg
```

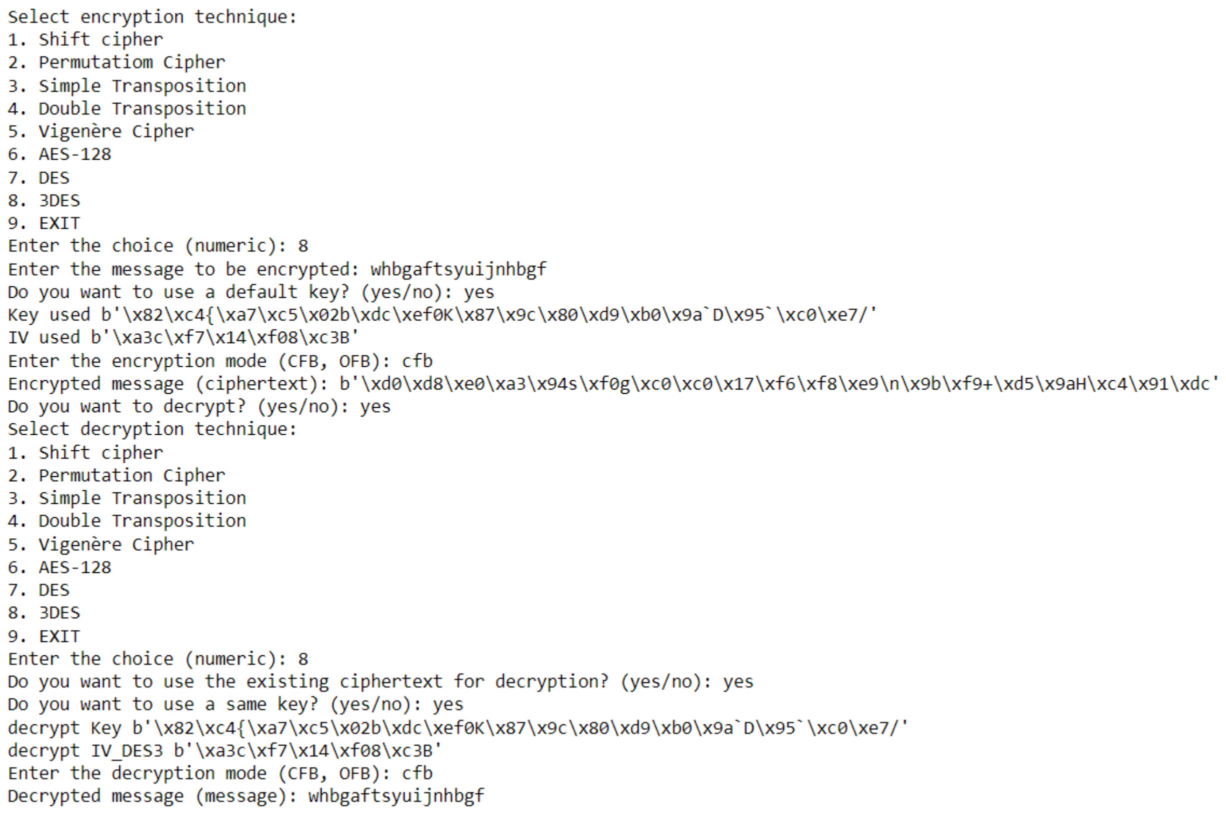
Case2: OFB



```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 7
Enter the message to be encrypted: gahbcnjdhytefsghbv
Do you want to use a default key? (yes/no): yes
Key used b'\xeb\x8d\xea\xc8\xc5\xb6\x08\xb2'
IV used b'P\xd4%\\H\xc6:,'
Enter the encryption mode (CFB, OFB): ofb
Encrypted message (ciphertext): b'#\xe9\xbd\x96\x9d\x8d\x04\xdeh\xcc\xf5\x82u\xd6\x86\x87\x93\x89OV;\x07\xd5\x89'
Do you want to decrypt? (yes/no): yes
Select decryption technique:
1. Shift cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 7
Do you want to use the existing ciphertext for decryption? (yes/no): yes
Do you want to use a same key? (yes/no): yes
decrypt Key b'\xeb\x8d\xea\xc8\xc5\xb6\x08\xb2'
decrypt IV_DES b'P\xd4%\\H\xc6:,'
Enter the decryption mode (CFB, OFB): ofb
Decrypted message (message): gahbcnjdhytefsghbv
```

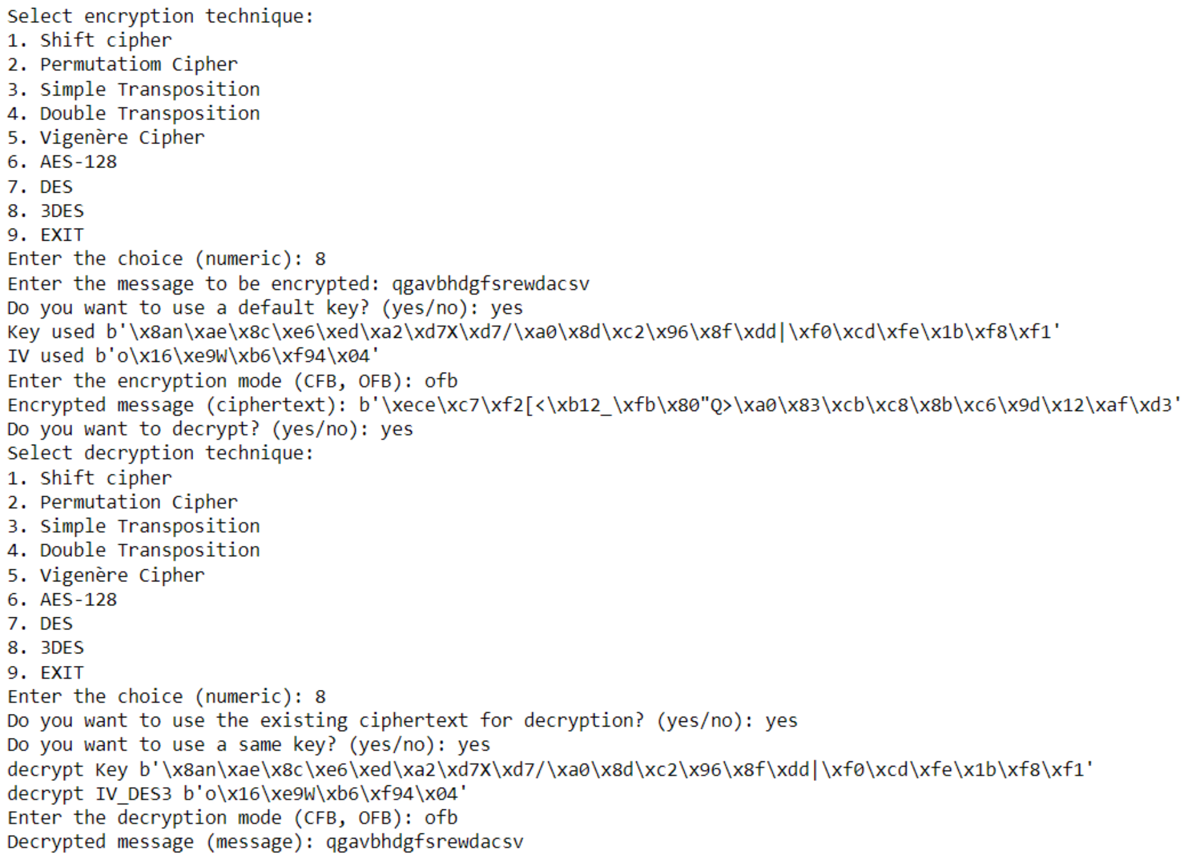
For (choice: 8 – 3DES)

Case1: CFB



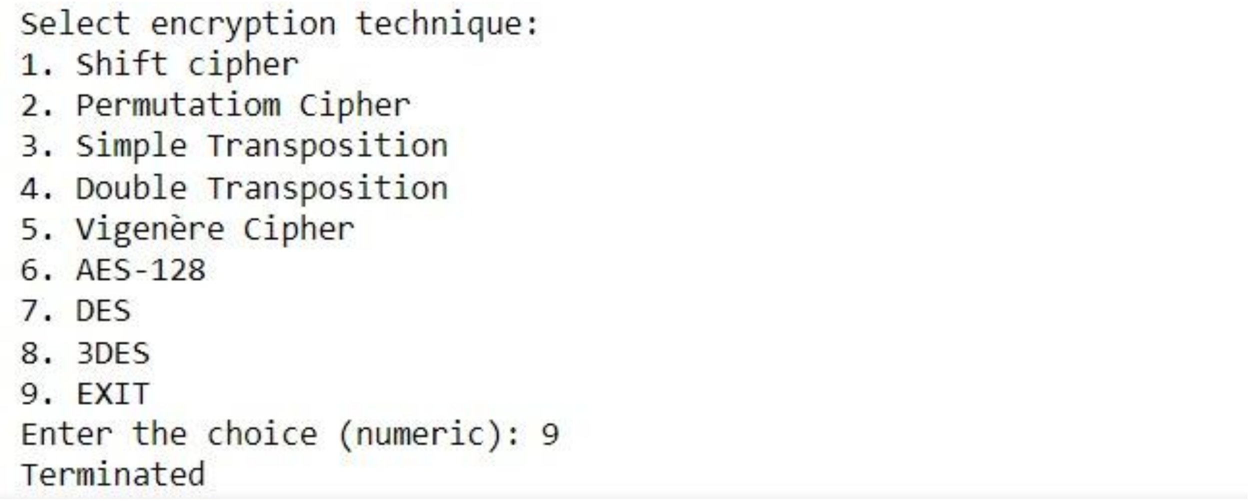
```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 8
Enter the message to be encrypted: whbgaftsyuijnhbgf
Do you want to use a default key? (yes/no): yes
Key used b'\x82\xc4{\xa7\xc5\x02b\xdc\xef0K\x87\x9c\x80\xd9\xb0\x9a`D\x95`\xc0\xe7/'
IV used b'\xa3c\xf7\x14\xf08\xc3B'
Enter the encryption mode (CFB, OFB): cfb
Encrypted message (ciphertext): b'\xd0\xd8\xe0\xa3\x94s\xf0g\xc0\xc0\x17\xf6\xf8\xe9\n\x9b\xf9+\xd5\x9aH\xc4\x91\xdc'
Do you want to decrypt? (yes/no): yes
Select decryption technique:
1. Shift cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 8
Do you want to use the existing ciphertext for decryption? (yes/no): yes
Do you want to use a same key? (yes/no): yes
decrypt Key b'\x82\xc4{\xa7\xc5\x02b\xdc\xef0K\x87\x9c\x80\xd9\xb0\x9a`D\x95`\xc0\xe7/'
decrypt IV_DES3 b'\xa3c\xf7\x14\xf08\xc3B'
Enter the decryption mode (CFB, OFB): cfb
Decrypted message (message): whbgaftsyuijnhbgf
```

Case2: OFB



```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 8
Enter the message to be encrypted: qgavbhdgfsrewdacsv
Do you want to use a default key? (yes/no): yes
Key used b'\x8an\xae\x8c\xe6\xed\xa2\xd7X\xd7/\xa0\x8d\xc2\x96\x8f\xdd|\xf0\xcd\xfe\x1b\xf8\xf1'
IV used b'o\x16\xe9W\xb6\xf94\x04'
Enter the encryption mode (CFB, OFB): ofb
Encrypted message (ciphertext): b'\xece\xc7\xf2[<\xb12_\xfb\x80"Q>\xa0\x83\xcb\xc8\x8b\xc6\x9d\x12\xaf\xd3'
Do you want to decrypt? (yes/no): yes
Select decryption technique:
1. Shift cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 8
Do you want to use the existing ciphertext for decryption? (yes/no): yes
Do you want to use a same key? (yes/no): yes
decrypt Key b'\x8an\xae\x8c\xe6\xed\xa2\xd7X\xd7/\xa0\x8d\xc2\x96\x8f\xdd|\xf0\xcd\xfe\x1b\xf8\xf1'
decrypt IV_DES3 b'o\x16\xe9W\xb6\xf94\x04'
Enter the decryption mode (CFB, OFB): ofb
Decrypted message (message): qgavbhdgfsrewdacsv
```

For 9(choice: 9 – EXIT)



```
Select encryption technique:
1. Shift cipher
2. Permutatiom Cipher
3. Simple Transposition
4. Double Transposition
5. Vigenère Cipher
6. AES-128
7. DES
8. 3DES
9. EXIT
Enter the choice (numeric): 9
Terminated
```