NAME: MANSI PATIL
CWID: A20549858

CS 458 Spring 2024 - Coding assignment II

Program Features:

1. Substitution cipher
   - Shift Cipher
   - Permutation Cipher
2. Transposition ciphers
   - Simple Transposition
   - Double Transposition
3. Vigenere Cipher
4. Different encryption algorithms (e.g., AES-128, DES, 3DES)
5. Different encryption modes (e.g., ECB, CBC, CFB, OFB)

Encryption is the process of encoding information to secure it from unauthorized access or use.

Substitution ciphers, such as the Shift Cipher and Permutation Cipher, involve replacing plaintext characters with other characters according to a defined rule.

Transposition ciphers, including Simple Transposition and Double Transposition, rearrange the order of characters in the plaintext.

The Vigenère Cipher is a polyalphabetic substitution cipher that uses a keyword to determine the shifting of letters.

In modern cryptography, different encryption algorithms like AES-128, DES (Data Encryption Standard), and 3DES (Triple DES) are widely used to encrypt data.

These algorithms are complemented by different encryption modes such as ECB (Electronic Codebook), CBC (Cipher Block Chaining), CFB (Cipher Feedback), and OFB (Output Feedback), which dictate how the encryption process is applied to blocks of data.

Each combination of algorithm and mode offers unique strengths and considerations in terms of security and efficiency.

The basic terminology of crypto includes the following:

Cipher: a particular algorithm (cryptographic system)
Plaintext: original message
Ciphertext: encrypted or coded message
Encryption: convert from plaintext to ciphertext (enciphering)
Decryption: restore the plaintext from ciphertext (deciphering)
Key: critical information used in cipher known only to sender/receiver
Symmetric: key cryptosystem uses the same key to encrypt as to decrypt

SUBSTITUTION CIPHER (SHIFT CIPHER)

- With a shift of 10, every letter is replaced by the letter 10 letters to its right.
- Deciphering is done in reverse, with a left shift of 10.
- For Example: It shifts letters by a fixed number of positions, like shifting "A" to "D" with a shift of 3.

- Decrypting the message using key.

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 1
The Substitution Cipher has been selected.
Pick a shift or permutation technique for the substitution cipher.(shift or permutation): shift
Type the content that you want to encrypt.: The secret to creativity is knowing how to hide your sources
Enter the shift value: 10
Encrypted Message: Dro combod dy mbokdsfsdi sc uxygsxq ryg dy rsno iyeb cyebmoc
Would you like to decrypt this message? (yes or no): yes
 Which would you prefer-using the ciphertext or a key for decryption?(key/ciphertext): key
Enter the decryption's shift value : 10
Decrypted Message: The secret to creativity is knowing how to hide your sources
```

- It will be encrypted by a shift of 15
- Decrypting the message using ciphertext.

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 1
The Substitution Cipher has been selected.
Pick a shift or permutation technique for the substitution cipher.(shift or permutation): shift
Type the content that you want to encrypt.:  love coding with Python
Enter the shift value: 15
Encrypted Message:  adkt rdsxcv lxiw Eniwdc
Would you like to decrypt this message? (yes or no): yes
 Which would you prefer-using the ciphertext or a key for decryption?(key/ciphertext): ciphertext
To decrypt, enter the ciphertex.: adkt rdsxcv lxiw Eniwdc
Decrypted Message: love coding with Python
```

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 1
The Substitution Cipher has been selected.
Pick a shift or permutation technique for the substitution cipher.(shift or permutation): shift
Type the content that you want to encrypt.: The shift cipher encryption uses an alphabet and a key that shifts the position of its letters.
Enter the shift value: 9
Encrypted Message: Cqn bqroc lryqna nwlahycrxw dbnb jw juyqjknc jwm j tnh cqjc bqrocb cqn yxbrcrxw xo rcb unccnab.
Would you like to decrypt this message? (yes or no): yes
 Which would you prefer-using the ciphertext or a key for decryption?(key/ciphertext): ciphertext
To decrypt, enter the ciphertex.: Cqn bqroc lryqna nwlahycrxw dbnb jw juyqjknc jwm j tnh cqjc bqrocb cqn yxbrcrxw xo rcb unccnab.
Decrypted Message: The shift cipher encryption uses an alphabet and a key that shifts the position of its letters.
```

SUBSTITUTION CIPHER (PERMUTATION CIPHER)

- The secret key for this cipher is a randomly chosen permutation of the numbers from 0 to 25, which correspond to the letters of the alphabet.
- Since the permutation key is a mapping of all 26 letters of the alphabet, there are 26! (26 factorial) possible permutations.
- Can be used for simple encryption tasks or educational purposes due to its straightforward implementation

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 1
The Substitution Cipher has been selected.
Pick a shift or permutation technique for the substitution cipher.(shift or permutation): Permutation
Type the content that you want to encrypt.: I love coding with Python
Encrypted Message: O rhnd qhloma zobp Xwbphm
Do you want to decrypt this message? (yes/no): yes
Decrypted Message: P cxef hxjpym opvw Tuvwxy
```

- Every time it will give different encrypted message.

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 1
The Substitution Cipher has been selected.
Pick a shift or permutation technique for the substitution cipher.(shift or permutation): permutation
Type the content that you want to encrypt.: I Love coding with Python
Encrypted Message: C Lqek ngactx jcgp Zmgpqt
```

TRANSPOSITION CIPHER
(SIMPLE TRANSPOSITION AND DOUBLE TRANSPOSITION)

- The name given to any encryption that involves rearranging the plaintext letters in a new order i.e., rearrange characters of plaintext to produce ciphertext.
- Key is the matrix size and the row and column permutations.
- Usage: Simple Transposition can be used for basic encryption needs where security requirements are not stringent, such as hiding messages in puzzles or games.
- The double-layered encryption adds an extra level of security compared to Simple Transposition.
- Usage: Double Transposition can be used when a higher level of security is required, such as in military communications or secure messaging applications.

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 2
You have selected Transposition Ciphers.
Choose Transposition Cipher technique (simple/double): simple
Enter the message that you want to encrypted: Hello Mansi
Enter the key for simple transposition: 21345 45321
Encrypted Message:  eiHslnlMoa
Do you want to decrypt this message? (yes/no): yes
Decrypted Message: Hello Mansi
```

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 2
You have selected Transposition Ciphers.
Choose Transposition Cipher technique (simple/double): double
Enter the message that you want to encrypted: HELLO MANSU
For double transposition, Enter the first key: 53214 23145
For double transposition, Enter the second key: 41235 54132
Encrypted Message: ELSNULH OMA
Do you want to decrypt this message? (yes/no): yes
Decrypted Message: HELLO MANSU
```

VIGENÈRE CIPHER

- The Vigenère cipher is a polyalphabetic cipher in which the number of different substitutions r is also part of the key.
- The Vigenère cipher uses a 26×26 table with A to Z as the row heading and column heading.
- Its security is considered weak by modern standards due to its vulnerability to frequency analysis and other cryptographic attacks.

- Decrypting using key.

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 3
You've chosen Vigenère Cipher.
Enter the message to encrypt: Learning never exhausts the mind
Enter the key for Vigenère Cipher: KEY
Encrypted Message: Viybrgxk xitov obfkyqdw dlc qgxh
Do you want to decrypt this message? (yes/no): YES
Which would you prefer- ciphertext or a key for decryption? (key/ciphertext): key
Enter the key for decryption: KEY
Decrypted Message: Learning never exhausts the mind
```

- Decrypting using Ciphertext

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 3
You've chosen Vigenère Cipher.
Enter the message to encrypt: Learning never exhausts the mind
Enter the key for Vigenère Cipher: IITC
Encrypted Message: Tmttvqgi vxxmz gfptwabl bpx uqgf
Do you want to decrypt this message? (yes/no): yes
Which would you prefer- ciphertext or a key for decryption? (key/ciphertext): ciphertext
Enter the ciphertext to decrypt: Tmttvqgi vxxmz gfptwabl bpx uqgf
Decrypted Message: Learning never exhausts the mind
```

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 3
You've chosen Vigenère Cipher.
Enter the message to encrypt: Hello Mansi
Enter the key for Vigenère Cipher: my
Encrypted Message: Tcxja Yyzqu
Do you want to decrypt this message? (yes/no): yes
Which would you prefer- ciphertext or a key for decryption? (key/ciphertext):
Your selection is invalid
```

AES-128(ECB MODE)

- AES 128 is an example of a symmetric encryption technique that uses the same cryptographic key to encrypt and decrypt data.
- The key used in AES-128 is 128 bits long(16byte).
- In ECB mode, AES-128 encrypts each block independently.
- Widely adopted for securing sensitive data in various applications such as banking, e-commerce, and government communications due to its high level of security and efficiency.

- Using Default key for both encryption and decryption

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): AES-128
Enter encryption mode (ECB, CBC): ECB
Enter the message that you want to encrypted: Hello Friends
Would you prefer to enter a custom key? (yes/no): no
Using the default key.: Thisis16-bytekey
Encrypted Message: GdvXN0G+RSYBKPqm6fv5sA==
Do you want to decrypt this message? (yes/no): yes
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): key
Do you want to use a custom key or default key? (custom/default): default
Decrypted Message: Hello Friends
```

- Using custom key for Encryption and default key for Decryption (SAME KEY)

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): AES-128
Enter encryption mode (ECB, CBC): ECB
Enter the message that you want to encrypted: ATTACKATSCHOOL
Would you prefer to enter a custom key? (yes/no): YES
Enter the encryption key: MYNAMEISMANSIPAT
Encrypted Message: K6i5AT1t/8Wx1BMdv7D0mQ==
Do you want to decrypt this message? (yes/no): YES
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): KEY
Do you want to use a custom key or default key? (custom/default): DEFAULT
Decrypted Message: ATTACKATSCHOOL
```

- Using default key for Encryption and ciphertext for Decryption

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): AES-128
Enter encryption mode (ECB, CBC): ECB
Enter the message that you want to encrypted: ATTACK
Would you prefer to enter a custom key? (yes/no): no
Using the default key.: Thisis16-bytekey
Encrypted Message: nfYaAcXqod0PHfKihVwCIg==
Do you want to decrypt this message? (yes/no): yes
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): ciphertext
Enter the ciphertext to decrypt: nfYaAcXqod0PHfKihVwCIg==
Decrypted Message: ATTACK
```

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): AES-128
Enter encryption mode (ECB, CBC): ECB
Enter the message that you want to encrypted: Confidential Data
Would you prefer to enter a custom key? (yes/no): NO
Using the default key.: Thisis16-bytekey
Encrypted Message: VEL0eI8zzOojYuY7VcnZbttVND0BSRmCVOnvv3jkkn0=
Do you want to decrypt this message? (yes/no): YES
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext):
Please try again. Your choice is invalid..
```

AES-128(CBC MODE)

- In, CBC mode, each plaintext block is XORed with the previous ciphertext block before encryption.
- The default key used in AES-128 is 128 bits long(16byte).
- Using default key for Encryption and Decryption.

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): AES-128
Enter encryption mode (ECB, CBC): CBC
Enter the message that you want to encrypted: Top Secret Code
Would you prefer to enter a custom key? (yes/no): NO
Using the default key.: Thisis16-bytekey
Encrypted Message: xK8xGCc3ZKTpz9/Q1tyNldKSaxPMrenEsindHZuUQUk=
Do you want to decrypt this message? (yes/no): YES
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): KEY
Do you want to use a custom key or default key? (custom/default): DEFAULT
Decrypted Message: Top Secret Code
```

- Using custom key for Encryption and decryption

```
Decrypted Message: SECRET

 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): aes-128
Enter encryption mode (ECB, CBC): cbc
Enter the message that you want to encrypted: Hidden message
Would you prefer to enter a custom key? (yes/no): yes
Enter the encryption key: mynameismansupat
Encrypted Message: UGSHvUwKyxBeSJSi7tzrN2175sLVQTUWTYv8mKN1v8Q=
Do you want to decrypt this message? (yes/no): yes
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): key
Do you want to use a custom key or default key? (custom/default): custom
Enter the decryption key: mynameismansupat
Decrypted Message: Hidden message
```

- Using custom key for encryption and ciphertext for decryption

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): AES-128
Enter encryption mode (ECB, CBC): CBC
Enter the message that you want to encrypted: SECRET
Would you prefer to enter a custom key? (yes/no): YES
Enter the encryption key: MYNAMEISMANSUUUU
Encrypted Message: S2WW4fCyaGhDA4haowvZxaZ6Gvx8fROFOm+J6GKD/P8=
Do you want to decrypt this message? (yes/no): YES
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): CIPHERTEXT
Enter the ciphertext to decrypt: S2WW4fCyaGhDA4haowvZxaZ6Gvx8fROFOm+J6GKD/P8=
Decrypted Message: SECRET
```

- Message cannot be empty.

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): AES-128
Enter encryption mode (ECB, CBC): CBC
Enter the message that you want to encrypted:
Would you prefer to enter a custom key? (yes/no):
Using the default key.: Thisis16-bytekey
Error: Message cannot be empty, please enter the message.
```

- Key length must be 16 bytes

```
  Encryption Techniques:
 1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
 2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
 3. Vigenère Cipher
 4. Different encryption algorithms (AES-128, DES, 3DES)
 5. Different encryption modes (ECB, CBC)
 6. Exit
 Enter your choice: 4
 You've chosen Different encryption algorithms(AES-128,DES, 3DES).
 Enter the encryption algorithm (AES-128, DES, 3DES): AES-128
 Enter encryption mode (ECB, CBC): CBC
 Enter the message that you want to encrypted: TOP SECRET
 Would you prefer to enter a custom key? (yes/no): YES
 Enter the encryption key: HELLO
 The key's length is invalid. To use AES encryption, the key must be 16 bytes long.
```

DES

- DES is a block cipher that operates on 64-bit blocks of data.
- It uses a 56-bit key for encryption and decryption(8byte).
- Rarely used in modern applications due to its small key size and vulnerability to brute-force attacks. It's mainly of historical interest or in legacy systems.

DES (ECB mode)

- Using Default key for encryption and decryption

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): DES
Enter encryption mode (ECB, CBC): ECB
Enter the message that you want to encrypted: Confidential Data
Would you prefer to enter a custom key? (yes/no): NO
Using the default key.: 8bytekey
Encrypted Message: tZ4+0xNIV4opUnNBQdMAlXqOQmbEJUuI
Do you want to decrypt this message? (yes/no): YES
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): KEY
Do you want to use a custom key or default key? (custom/default): DEFAULT
Decrypted Message: Confidential Data
```

- It uses the same key for both encryption and decryption.

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): DES
Enter encryption mode (ECB, CBC): ECB
Enter the message that you want to encrypted: Confidential Data
Would you prefer to enter a custom key? (yes/no): YES
Enter the encryption key: QWERTYUI
Encrypted Message: 6Rrf2X1f17339Jh0zSZD+kIu3/cbNXPx
Do you want to decrypt this message? (yes/no): YES
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): KEY
Do you want to use a custom key or default key? (custom/default): CUSTOM
Enter the decryption key: QWERTYUI
Decrypted Message: Confidential Data
```

- Decryption using Ciphertext.

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): des
Enter encryption mode (ECB, CBC): ECB
Enter the message that you want to encrypted: secret
Would you prefer to enter a custom key? (yes/no): no
Using the default key.: 8bytekey
Encrypted Message: qkvzz2Z/fY8=
Do you want to decrypt this message? (yes/no): yes
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): ciphertext
Enter the ciphertext to decrypt: qkvzz2Z/fY8=
Decrypted Message: secret
```

- Key must be 8 bytes long

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): des
Enter encryption mode (ECB, CBC): ecb
Enter the message that you want to encrypted: hidden
Would you prefer to enter a custom key? (yes/no): yes
Enter the encryption key: 1sw
The key's length is invalid. To use DES encryption, the key must be 8 bytes long.
```

DES (CBC MODE)

- Using same key for encryption and decryption

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): des
Enter encryption mode (ECB, CBC): CBC
Enter the message that you want to encrypted: Encrypted Data
Would you prefer to enter a custom key? (yes/no): no
Using the default key.: 8bytekey
Encrypted Message: O7BwhF3Gor4pNJnzf9g9gGiK6EuI3xQ2
Do you want to decrypt this message? (yes/no): yes
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): key
Do you want to use a custom key or default key? (custom/default): default
Decrypted Message: Encrypted Data
```

- Using custom key for Encryption and decryption(8byte).

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): des
Enter encryption mode (ECB, CBC): cbc
Enter the message that you want to encrypted: Secure Communication
Would you prefer to enter a custom key? (yes/no): yes
Enter the encryption key: 12345678
Encrypted Message: Sl2+8C0oJGAIB3K0cl28mZ/LmuOTcMYANaz82TtYDIE=
Do you want to decrypt this message? (yes/no): yes
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): key
Do you want to use a custom key or default key? (custom/default): custom
Enter the decryption key: 12345678
Decrypted Message: Secure Communication
```

- Using default key for Encryption and ciphertext for Decryption

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): des
Enter encryption mode (ECB, CBC): cbc
Enter the message that you want to encrypted: secure
Would you prefer to enter a custom key? (yes/no): no
Using the default key.: 8bytekey
Encrypted Message: KO6A9aGvo2w5bb0m6ak9vg==
Do you want to decrypt this message? (yes/no): yes
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): ciphertext
Enter the ciphertext to decrypt: KO6A9aGvo2w5bb0m6ak9vg==
Decrypted Message: secure
```

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): des
Enter encryption mode (ECB, CBC): cbc
Enter the message that you want to encrypted:
Would you prefer to enter a custom key? (yes/no):
Using the default key.: 8bytekey
Error: Message cannot be empty, please enter the message.
```

3DES

- 3DES uses three keys and three executions of the DES algorithm.
- 3 keys, 168 bits key length(24byte).

3DES (ECB)

- Using same default key for Encryption and decryption.

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): 3des
Enter encryption mode (ECB, CBC): ecb
Enter the message that you want to encrypted: Confidential Files
Would you prefer to enter a custom key? (yes/no): no
Using the default key.: This is a 24-byte 3DESke
Encrypted Message: Ez8sCKGnRstxJJv2gzQgn29uaIkS2Qh2
Do you want to decrypt this message? (yes/no): yes
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): key
Do you want to use a custom key or default key? (custom/default): default
Decrypted Message: Confidential Files
```

- Using custom key for Encryption and Decryption.
- Using same key for both Encryption and decryption.

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): 3des
Enter encryption mode (ECB, CBC): ecb
Enter the message that you want to encrypted: Private message
Would you prefer to enter a custom key? (yes/no): yes
Enter the encryption key: qwertyuiopasdfghjklzxcvb
Encrypted Message: 6B7DJasZxv33ym5D3PKVxA==
Do you want to decrypt this message? (yes/no): yes
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): key
Do you want to use a custom key or default key? (custom/default): custom
Enter the decryption key: qwertyuiopasdfghjklzxcvb
Decrypted Message: Private message
```

- Key cannot be empty and must be 24 bytes long.

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): 3des
Enter encryption mode (ECB, CBC): ecb
Enter the message that you want to encrypted: Confidential Files
Would you prefer to enter a custom key? (yes/no): yes
Enter the encryption key:
The key's length is invalid. To use 3DES encryption, the key must be 24 bytes long
```

Must be same key

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): 3des
Enter encryption mode (ECB, CBC): ecb
Enter the message that you want to encrypted: Private Key
Would you prefer to enter a custom key? (yes/no): yes
Enter the encryption key: hell is a qw erte 3dewas
Encrypted Message: dPdZ8hc0+cxOPBcZKkniDw==
Do you want to decrypt this message? (yes/no): yes
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): key
Do you want to use a custom key or default key? (custom/default): custom
Enter the decryption key: dPdZ8hc0+cxOPBcZKkniDw==
Error: Padding is incorrect.
```

3DES(CBC)

- Using default key for both encryption and decryption

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): 3des
Enter encryption mode (ECB, CBC): cbc
Enter the message that you want to encrypted: private
Would you prefer to enter a custom key? (yes/no): no
Using the default key.: This is a 24-byte 3DESke
Encrypted Message: FX7Q1yx1U99cVhRc9e4jUA==
Do you want to decrypt this message? (yes/no): yes
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): key
Do you want to use a custom key or default key? (custom/default): default
Decrypted Message: private
```

- Using custom key for Encryption and Decryption.

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): 3des
Enter encryption mode (ECB, CBC): cbc
Enter the message that you want to encrypted: private message: attackatdawn
Would you prefer to enter a custom key? (yes/no): yes
Enter the encryption key: 1234567890qwertyuiopasdf
Encrypted Message: eLI+f2MaMhGh6i4QJwob835eT7mBGcx6jRYFcN7fFtWvpGzmAcVX1A==
Do you want to decrypt this message? (yes/no): yes
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): key
Do you want to use a custom key or default key? (custom/default): custom
Enter the decryption key: 1234567890qwertyuiopasdf
Decrypted Message: private message: attackatdawn
```

- Using ciphertext for decryption

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): 3des
Enter encryption mode (ECB, CBC): cbc
Enter the message that you want to encrypted: Restricted Access
Would you prefer to enter a custom key? (yes/no): no
Using the default key.: This is a 24-byte 3DESke
Encrypted Message: 8E97JiFTvAQkDUIgSc0rPB7kxTr+7hRtPkTp6KJjmzc=
Do you want to decrypt this message? (yes/no): yes
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext): ciphertext
Enter the ciphertext to decrypt: 8E97JiFTvAQkDUIgSc0rPB7kxTr+7hRtPkTp6KJjmzc=
Decrypted Message: Restricted Access
```

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): 3des
Enter encryption mode (ECB, CBC): cbc
Enter the message that you want to encrypted: private private private private
Would you prefer to enter a custom key? (yes/no): no
Using the default key.: This is a 24-byte 3DESke
Encrypted Message: kLp19ptTfbE5Mn+5pBFK4lXEuh2wo+AqwuHEpYHRG5rGLNuGVLNYHw==
Do you want to decrypt this message? (yes/no): yes
Which would you prefer-using the ciphertext or a key for decryption? (key/ciphertext):
Please try again. Your choice is invalid..
```

```
  Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 4
You've chosen Different encryption algorithms(AES-128,DES, 3DES).
Enter the encryption algorithm (AES-128, DES, 3DES): 3des
Enter encryption mode (ECB, CBC): cbc
Enter the message that you want to encrypted: private private private private
Would you prefer to enter a custom key? (yes/no): yes
Enter the encryption key: 1wsw34de4
The key's length is invalid. To use 3DES encryption, the key must be 24 bytes long
```

- ECB (Electronic Codebook) and CBC (Cipher Block Chaining) are modes of operation used in block cipher algorithms like DES or AES to provide confidentiality when encrypting data.

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 5
Option 4 is interconnected with this option. To use different encryption modes with different encryption methods, please select option 4.
```

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 7
Invalid choice. Please try again.
```

```
 Encryption Techniques:
1. Substitution Cipher
        - Shift Cipher
        - Permutation Cipher
2. Transposition Ciphers
        - Simple Transposition
        - Double Transposition
3. Vigenère Cipher
4. Different encryption algorithms (AES-128, DES, 3DES)
5. Different encryption modes (ECB, CBC)
6. Exit
Enter your choice: 6
Exiting program.
Exit the loop and end the program
```