

Name: Deep Pawar(A20545137)
Professor: Yousef M Elmehdwi
Institute: Illinois Institute of Technology

CS 458: Introduction to Information Security

Spring 2024 - Coding Assignment 2

OBJECTIVE:

The objective of this assignment is to implement a command-line program in a language of your choice that allows users to perform encryption and decryption using various techniques covered in lab 2, including substitution ciphers, transposition ciphers, different encryption algorithms, and modes.

PROGRAM FEATURES:

1. The program should display a list of options for encryption techniques, including:
 - i. Substitution cipher:
 - a. Shift Cipher
 - b. Permutation Cipher
 - ii. Transposition ciphers
 - a. Simple Transposition
 - b. Double Transposition
 - iii. Vigenere Cipher
 - iv. Different encryption algorithms (e.g., AES-128, DES, 3DES)
 - v. Different encryption modes (e.g., ECB, CBC, CFB, OFB)
2. Based on the user's selection, prompt the user to enter a message (plaintext) to be encrypted.
3. The size of the message should be greater than the maximum size of the block used by the chosen encryption algorithm.
4. After entering the message, allow the user to choose whether to enter an encryption key or use a default key.
5. Perform the encryption using the selected technique and encryption key.
6. Display the encrypted message (ciphertext).
7. Provide an option for decryption, where the user can input the ciphertext and select the appropriate decryption technique based on the encryption method used.
8. If decryption is selected, prompt the user to enter the decryption key or use the same key as encryption by default.
9. Perform decryption using the selected technique and decryption key.
10. Display the decrypted message (plaintext).

SUBMISSION:

Submit the source code of your program along with a brief report describing the functionality, usage instructions, and any observations or challenges encountered during the implementation. Include screenshots demonstrating the encryption and decryption processes using different techniques. Upload the files to the course Blackboard for evaluation.

NOTE: The Professor told us to use any two of the encryption modes, so I have used ECB and CBC modes in this assignment.

- **Encryption Techniques:**

1. Substitution cipher:

A secret key is used to map each letter of the alphabet to a corresponding replacement letter or symbol in a substitution cipher. The substitution cipher converts unencrypted text, or plaintext, into publicly accessible encrypted text, or ciphertext. We need to use the same key to reverse the substitution process to decrypt the ciphertext and retrieve the original plaintext.

a. Shift Cipher:

The Caesar Cipher, sometimes referred to as the Shift Cipher involves moving each letter in the plaintext up or down the alphabet by a certain amount. Usually, a key that is an integer that indicates how many positions each letter is shifted is used to express this shift. Shift ciphers are easy to use and comprehend, but they can also be easily cracked by frequency analysis or brute force techniques, particularly when the key space is limited. As a result, their main applications are in educating or as parts of more intricate encryption schemes.

b. Permutation Cipher:

A permutation cipher, sometimes referred to as a transposition cipher, is a kind of encryption in which the plaintext's character locations are rearranged according to a specific permutation or rule. Permutation Ciphers change the plaintext's character order without altering the characters themselves, as opposed to Substitution Ciphers, which swap out letters.

2. Transposition ciphers:

Transposition ciphers are a sort of encryption method in which the plaintext's character locations are rearranged according to a system or key. Transposition ciphers just need to rearrange the characters, as opposed to substitution ciphers, which switch out the characters for different ones. Transposition ciphers come in a variety of forms, but they always have the trait of changing the plaintext characters' locations.

a. Simple Transposition:

A Simple Transposition Cipher is a type of encryption used in cryptography where the ciphertext is created by rearranging the plaintext's character locations by a predetermined scheme or pattern. Transposition ciphers alter the characters' sequence of appearance rather than the characters themselves. The plaintext is split into fixed-length blocks, typically rows, in a simple transposition cipher. The characters within each block are then rearranged by a predetermined pattern. The pattern may entail changing the characters in each block, changing the blocks' order, or doing both.

These ciphers can be easily implemented and understood, they are vulnerable to cryptanalysis techniques like frequency analysis, particularly if the transposition pattern is predictable. To increase security, they are frequently used in conjunction with other cryptographic methods.

b. Double Transposition:

In Double Transposition, to encrypt a message, the transposition function (rearranging the character order) must be used twice. The encrypted message is the resultant ciphertext of the Double Transposition process, which introduces an additional layer of complexity to the encryption process, making it more secure than a single transposition or straightforward substitution cipher. The ciphertext is converted twice in reverse order to yield the original plaintext message, which is then used to decrypt the message.

3. Vigenere Cipher:

A basic polyalphabetic substitution technique is used in the Vigenère cipher to encrypt alphabetic text. As alphabetic refers to "having to do with the alphabet," and poly meaning "many," polyalphabetic refers to "many alphabets." To match the length of the plaintext message, a keyword is repeated in the Vigenère encryption. The shift values for each letter in the keyword are corresponding. The matching letters of the plaintext message are shifted cyclically by the alphabetical order using these shift values.

For a very long time, the Vigenère cipher was thought to be unbreakable due to its ability to conceal letter frequencies and withstand frequency analysis, which was the most popular technique for cracking ciphers at the time. However, it is susceptible to several types of cryptanalysis, particularly if the keyword is known or easily guessed.

- **Encryption Algorithms:**

1. AES-128:

Symmetric encryption algorithms like AES-128 are often used to protect sensitive data. AES stands for Advanced Encryption Standard. AES works with data blocks, which are made up of 128 bits (16 bytes) apiece. The technique encrypts plaintext data using a sequence of substitution, permutation, and mixing operations called rounds. In a process known as "substitution-permutation network," bytes are substituted using a substitution box (S-box) and then shuffled using permutation techniques to process the input data during encryption. This procedure is carried out in numerous rounds (10 rounds for AES-128), using a distinct set of operations in each cycle.

The efficiency and security of AES-128 is one of its main advantages. When used with a strong key, it is considered to be extremely secure against a variety of cryptographic attacks. AES is also computationally efficient, which makes it appropriate for usage in a variety of applications. These applications include safeguarding confidential data, preserving data confidentiality, and securing data transfer over the Internet.

2. DES:

The symmetric-key block cipher method known as DES (Data Encryption Standard) was extensively used in the encryption of electronic data. Using a 56-bit key, the method runs on 64-bit plaintext blocks. The plaintext is split up into blocks during the encryption process, and depending on the key, each block is subjected to several changes, such as transposition, substitution, and permutation. From the original 56-bit key, the key schedule creates 16 48-bit subkeys, which are used in the encryption rounds. The ciphertext block that is generated is the result of 16 operation rounds.

Even while DES was widely used at first, increases in processing power allowed for exhaustive key search attacks, which made DES less safe over time. However, DES continues to have an impact on the cryptography community as it provided the foundation for other block cipher algorithms and cryptographic standards that came after. With larger key sizes and more intricate processes, its replacement, the Advanced Encryption Standard (AES), was chosen through an open competition and provides noticeably improved security, making it appropriate for contemporary cryptographic applications.

3. 3DES:

The Triple Data Encryption Standard (3DES) was created to offer more security than Data Encryption Standard (DES). Using two or three separate keys, the DES algorithm is applied three times to each data block in the 3DES scheme. It functions in a variety of ways, including Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Electronic Codebook (ECB). 3DES uses the DES algorithm three times in succession to encrypt or decrypt data in fixed-size blocks of 64 bits in each mode. While the second application of DES always uses the opposite key, the first and third applications can utilize the same or different keys.

Even while 3DES offered more security than DES, it is currently regarded as being slower and less effective than more recent encryption algorithms like AES (Advanced Encryption Standard). Because it makes use of three distinct 56-bit keys, its key length is 168 bits. However, the effective security strength is weakened by the use of three rounds of encryption, leaving it vulnerable to some kinds of attacks. Because AES provides better performance and stronger security, many organizations have switched to it as their preferred symmetric-key encryption technique. However, 3DES is still in use in some outdated systems due to backward compatibility or other security considerations.

- **Encryption Modes:**

1. ECB

A fundamental encryption mode used in block cipher techniques is called ECB (Electronic Codebook) mode. In ECB mode, the same encryption key is used to independently encrypt each plaintext block. This implies that blocks of ciphertext generated from identical plaintext blocks will also be similar. Because patterns from the plaintext may still be discernible in the ciphertext, this lack of randomization in the encryption process might result in problems. Furthermore, there is no dispersion of faults because every block is encrypted separately; if one block becomes faulty during storage or transmission, it will only impact that specific block and not the others. Because ECB mode is straightforward and effective, it can be used in situations when error diffusion and randomness are not important.

2. CBC

One popular mode of operation for block ciphers such as AES (Advanced Encryption Standard) is Cipher Block Chaining (CBC). Each plaintext block in CBC mode is encrypted after being merged with the previous block's ciphertext. By adding a diffusion element, this chaining mechanism reduces its vulnerability to some attacks. To add randomization and make sure that identical plaintext blocks do not result in the same ciphertext blocks, an initialization vector (IV) is first XORed with the first plaintext block. Before encryption, the current plaintext block and the ciphertext of the preceding block are XORed for consecutive blocks. This chaining approach improves security by ensuring that even slight modifications to the plaintext produce radically different ciphertexts.

- **Workflow of the Code:**

- **Importing Libraries:**

The code begins by importing necessary libraries from the Crypto module, including modules for various encryption algorithms and utilities.

- **Substitution Shift Cipher Encryption Function:**

Defines a function `substitution_shift_cipher` to perform encryption using a shift cipher, where each letter in the message is shifted by a fixed number of positions in the alphabet.

- **Substitution Permutation Cipher Encryption Function:**

Defines a function `substitution_permutation_cipher` to perform encryption using a permutation cipher, where each letter in the message is substituted according to a given key.

- **Transposition Cipher (Simple) Encryption Function:**

Defines a function `transposition_cipher_simple_transposition` to perform encryption using a simple transposition cipher, where characters in the message are rearranged in a specific pattern.

- **Transposition Cipher (Double) Encryption Function:**

Defines a function `transposition_cipher_double_transposition` to perform encryption using a double transposition cipher, applying the simple transposition cipher twice.

- **Vigenere Cipher Encryption Function:**

Defines a function `vigenere_cipher` to perform encryption using a Vigenere cipher, which is a form of polyalphabetic substitution cipher.

- **AES, DES, and 3DES Encryption Functions:**

Defines functions for encryption using AES, DES, and 3DES encryption algorithms.

- **AES, DES, and 3DES Decryption Functions:**

Defines functions for decryption using AES, DES, and 3DES decryption algorithms.

- **Substitution Shift Cipher Decryption Function:**

Defines a function `substitution_shift_cipher_decrypt` for decrypting messages encrypted with the shift cipher.

- **Substitution Permutation Cipher Decryption Function:**

Defines a function `substitution_permutation_cipher_decrypt` for decrypting messages encrypted with the permutation cipher.

- **Transposition Cipher (Simple) Decryption Function:**

Defines a function `transposition_cipher_simple_transposition_decrypt` for decrypting messages encrypted with the simple transposition cipher.

- **Transposition Cipher (Double) Decryption Function:**

Defines a function `transposition_cipher_double_transposition_decrypt` for decrypting messages encrypted with the double transposition cipher.

- **Vigenere Cipher Decryption Function:**

Defines a function `vigenere_cipher_decrypt` for decrypting messages encrypted with the Vigenere cipher.

- **Main Function:**

The main function `main()` prompts the user to select an encryption technique, provides options to enter a message and necessary parameters, encrypts the message using the selected technique and encryption algorithm, and then optionally decrypts the encrypted message.

- **Execution:**

Finally, the code checks if it's being run as the main program and executes the `main()` function accordingly.

This workflow represents how the code allows users to encrypt messages using various encryption techniques and algorithms and optionally decrypt them using the same or compatible decryption techniques.

• Output:

- **Encryption Technique:** Substitution Cipher (Shift Cipher)
- **Encryption Algorithm:** AES-128
- **Encryption Mode:** ECB

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 1
Enter the message to be encrypted : deep pawar
Enter the shift key value : 4
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 1
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 1
The Encrypted Message (cipher_text) is : b'\xbaj\xd5\xe3l\x11tkI\xd05\xe2#\j\xdf\xc2'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 1
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 1
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 1
Enter the cipher_text : b'\xbaj\xd5\xe3l\x11tkI\xd05\xe2#\j\xdf\xc2'
Decrypted Message : hiit teaeav
Decrypted Message (plain_text) : deep pawar
>>>
Ln: 43 Col: 44

```

- **Encryption Technique:** Substitution Cipher (Shift Cipher)
- **Encryption Algorithm:** AES-128
- **Encryption Mode:** CBC

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 1
Enter the message to be encrypted : deep pawar
Enter the shift key value : 5
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 1
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 2
The Encrypted Message (cipher_text) is : b'\x18\x84\x83z\x87\xdaw\x08\xc7P\xed\x16/=m\x11'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 1
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 1
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 2
Enter the cipher_text : b'\x18\x84\x83z\x87\xdaw\x08\xc7P\xed\x16/=m\x11'
Decrypted Message : ijju ufbfw
Decrypted Message (plain_text) : deep pawar
>>>
Ln: 44 Col: 0

```

- **Encryption Technique:** Substitution Cipher (Shift Cipher)
- **Encryption Algorithm:** DES
- **Encryption Mode:** ECB

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 1
Enter the message to be encrypted : computer science
Enter the shift key value : 2
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 2
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 1
The Encrypted Message (cipher_text) is : b'3Y\x1d\x87\xec*\xf0\x88[\x9a\xf7\x9c?\x94\xc5\x8a6\x15r\xe1\x11\x01\xc2'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 1
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 2
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 1
Enter the cipher_text : b'3Y\x1d\x87\xec*\xf0\x88[\x9a\xf7\x9c?\x94\xc5\x8a6\x15r\xe1\x11\x01\xc2'
Decrypted Message : eqorwvgt uekgpeg
Decrypted Message (plain_text) : computer science
>>>
Ln: 44 Col: 0

```

- **Encryption Technique:** Substitution Cipher (Shift Cipher)
- **Encryption Algorithm:** DES
- **Encryption Mode:** CBC

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 1
Enter the message to be encrypted : computer science
Enter the shift key value : 3
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 2
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 2
The Encrypted Message (cipher_text) is : b'\K\xed\xad\xb8\xc8y\xed\x8b\x8a\x12\xbd\xa9\xd8\xf4\xda=k\xd6\xce}\x16U'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 1
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 2
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 2
Enter the cipher_text : b'\K\xed\xad\xb8\xc8y\xed\x8b\x8a\x12\xbd\xa9\xd8\xf4\xda=k\xd6\xce}\x16U'
Decrypted Message : frpsxwhu vflhqfh
Decrypted Message (plain_text) : computer science
>>>
Ln: 44 Col: 0

```


- **Encryption Technique:** Substitution Cipher (Shift Cipher)
- **Encryption Algorithm:** 3DES
- **Encryption Mode:** ECB

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 1
Enter the message to be encrypted : information security
Enter the shift key value : 6
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 3
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 1
The Encrypted Message (cipher_text) is : b"\xc07'E\xa0\x8c\xc2\xe6XW\xb3\xd6'\xceU\xba\xdlEU>\x88\x07\xbc5"
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 1
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 3
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 1
Enter the cipher_text : b"\xc07'E\xa0\x8c\xc2\xe6XW\xb3\xd6'\xceU\xba\xdlEU>\x88\x07\xbc5"
Decrypted Message : otluxsgzout ykiauxoze
Decrypted Message (plain_text) : information security
>>>
Ln: 44 Col: 0

```

- **Encryption Technique:** Substitution Cipher (Shift Cipher)
- **Encryption Algorithm:** 3DES
- **Encryption Mode:** CBC

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 1
Enter the message to be encrypted : information science
Enter the shift key value : 2
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 3
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 2
The Encrypted Message (cipher_text) is : b'J\n~\xd6p\x10\x86o}\xed{\x82Wos\xa2.f|l\xda\xcd\x9b\xe9'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 1
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 3
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 2
Enter the cipher_text : b'J\n~\xd6p\x10\x86o}\xed{\x82Wos\xa2.f|l\xda\xcd\x9b\xe9'
Decrypted Message : kphgtocvkqp uekgpeg
Decrypted Message (plain_text) : information science
>>>
Ln: 44 Col: 0

```

- **Encryption Technique:** Substitution Cipher (Permutation Cipher)
- **Encryption Algorithm:** AES-128
- **Encryption Mode:** ECB

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 2
Enter the message to be encrypted : cloud computing
Enter the permutation key value(26 characters) : qwertyuiopasdfghjklzxcvbnm
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 1
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 1
The Encrypted Message (cipher_text) is : b'\x94\xc7z\xbb\x01\x81\xe0^|R\xa7\x81\x0c\r5\xc0'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 2
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 1
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 1
Enter the cipher_text : b'\x94\xc7z\xbb\x01\x81\xe0^|R\xa7\x81\x0c\r5\xc0'
Decrypted Message : esgxr egdhxzofu
Decrypted Message (plain_text) : cloud computing
>>>
Ln: 3 Col: 0

```

- **Encryption Technique:** Substitution Cipher (Permutation Cipher)
- **Encryption Algorithm:** AES-128
- **Encryption Mode:** CBC

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 2
Enter the message to be encrypted : cloud computing
Enter the permutation key value(26 characters) : asdfghjklqwertyuiopzxcvbnm
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 1
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 2
The Encrypted Message (cipher_text) is : b'*\xb6\xaa\x8f\xb4\xa9_\x0e\xd0[\xd3&\xf9<\xef\x91'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 2
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 1
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 2
Enter the cipher_text : b'*\xb6\xaa\x8f\xb4\xa9_\x0e\xd0[\xd3&\xf9<\xef\x91'
Decrypted Message : deyxf dyruxzltj
Decrypted Message (plain_text) : cloud computing
>>>
Ln: 44 Col: 0

```

- **Encryption Technique:** Substitution Cipher (Permutation Cipher)
- **Encryption Algorithm:** DES
- **Encryption Mode:** ECB

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 2
Enter the message to be encrypted : Software Engineering
Enter the permutation key value(26 characters) : zxcvbnmqwertyuioasdfghjkl
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 2
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 1
The Encrypted Message (cipher_text) is : b'\xe8\xd6i\x82\x9a\x1f\xd4\x95\x07ALHh\xc17\xa9\xbd\xd8;&*\\\x15\xae'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 2
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 2
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 1
Enter the cipher_text : b'\xe8\xd6i\x82\x9a\x1f\xd4\x95\x07ALHh\xc17\xa9\xbd\xd8;&*\\\x15\xae'
Decrypted Message : Sindhazab Bumwubbawum
Decrypted Message (plain_text) : Software Engineering
>>>
Ln: 44 Col: 0

```

- **Encryption Technique:** Substitution Cipher (Permutation Cipher)
- **Encryption Algorithm:** DES
- **Encryption Mode:** CBC

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 2
Enter the message to be encrypted : software engineering
Enter the permutation key value(26 characters) : qazxswedcvfrtgbnhyujmkiolp
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 2
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 2
The Encrypted Message (cipher_text) is : b'5\xe5\xa8#\x02o\x02\x1d$g\xfaXVv\x0b\xd4V\xa7S!C9\x98}'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 2
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 2
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 2
Enter the cipher_text : b'5\xe5\xa8#\x02o\x02\x1d$g\xfaXVv\x0b\xd4V\xa7S!C9\x98}'
Decrypted Message : ubwjigys gsecgssycge
Decrypted Message (plain_text) : software engineering
>>>
Ln: 44 Col: 0

```

- **Encryption Technique:** Substitution Cipher (Permutation Cipher)
- **Encryption Algorithm:** 3DES
- **Encryption Mode:** ECB

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 2
Enter the message to be encrypted : machine learning
Enter the permutation key value(26 characters) : qweasdzxcrfvbgtyhnmjuiklop
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 3
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 1
The Encrypted Message (cipher_text) is : b'\x10\xb1\xd3<\xbc\xf4{"\x9a4:\xf2`\xa7\xb2\xc2\x86\x80}\xad\x9c\x12&9'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 2
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 3
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 1
Enter the cipher text : b'\x10\xb1\xd3<\xbc\xf4{"\x9a4:\xf2`\xa7\xb2\xc2\x86\x80}\xad\x9c\x12&9'
Decrypted Message : bqexcgs vsqngcgz
Decrypted Message (plain_text) : machine learning
>>>
Ln: 44 Col: 0

```

- **Encryption Technique:** Substitution Cipher (Permutation Cipher)
- **Encryption Algorithm:** 3DES
- **Encryption Mode:** CBC

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 2
Enter the message to be encrypted : machine learning
Enter the permutation key value(26 characters) : asdfghjklzxcvbnmqwertyuiop
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 3
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 2
The Encrypted Message (cipher_text) is : b'\xc50\xce"\x99\x81;\x8bC\xad\xbd5N\x11\xd9\x9a\xf8\x9e'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 2
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 3
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 2
Enter the cipher_text : b'\xc50\xce"\x99\x81;\x8bC\xad\xbd5N\x11\xd9\x9a\xf8\x9e'
Decrypted Message : vadklbg cgawblbj
Decrypted Message (plain_text) : machine learning
>>>
Ln: 44 Col: 0

```

- **Encryption Technique:** Transposition Cipher (Simple Transposition)
- **Encryption Algorithm:** AES-128
- **Encryption Mode:** ECB

```

Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 3
Enter the message to be encrypted : this is deep pawar
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 1
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 1
The Encrypted Message (cipher_text) is : b'\xad.0\x14\x91\x08GWG\xc9\xcb^y\xb5\xf2\xa5v)$C\xf0D\x8f\x1a\xb5\xef\x19\x899\x9eN\xe6'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 3
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 1
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 1
Enter the cipher_text : b'\xad.0\x14\x91\x08GWG\xc9\xcb^y\xb5\xf2\xa5v)$C\xf0D\x8f\x1a\xb5\xef\x19\x899\x9eN\xe6'
Decrypted Message : ti sde aahsi eppwr
Decrypted Message (plain_text) : this is deep pawar
>>>
Ln: 43 Col: 0

```

- **Encryption Technique:** Transposition Cipher (Simple Transposition)
- **Encryption Algorithm:** AES-128
- **Encryption Mode:** CBC

```

Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 3
Enter the message to be encrypted : this is deep pawar
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 1
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 2
The Encrypted Message (cipher_text) is : b'\xf9g[\xf3\xfdf#\x8e\xca\x98;\xb2p\xb9\xd0*96\xb9q\x84\xffs\xec\x92\x02\xf1\xbdEn\x11\xa9'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 3
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 1
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 2
Enter the cipher_text : b'\xf9g[\xf3\xfdf#\x8e\xca\x98;\xb2p\xb9\xd0*96\xb9q\x84\xffs\xec\x92\x02\xf1\xbdEn\x11\xa9'
Decrypted Message : ti sde aahsi eppwr
Decrypted Message (plain_text) : this is deep pawar
>>>
Ln: 43 Col: 0

```

- **Encryption Technique:** Transposition Cipher (Simple Transposition)
- **Encryption Algorithm:** DES
- **Encryption Mode:** ECB

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 3
Enter the message to be encrypted : introduction to ml
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 2
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 1
The Encrypted Message (cipher_text) is : b'\xc4\xa6 \x14\x89L\xb5,\tx\xbc&`\xab\x07\xe4\xd6\x06\xbbg"<!\xed'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 3
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 2
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 1
Enter the cipher_text : b'\xc4\xa6 \x14\x89L\xb5,\tx\xbc&`\xab\x07\xe4\xd6\x06\xbbg"<!\xed'
Decrypted Message : itouto omnrdcint l
Decrypted Message (plain_text) : introduction to ml
>>>
Ln: 43 Col: 0

```

- **Encryption Technique:** Transposition Cipher (Simple Transposition)
- **Encryption Algorithm:** DES
- **Encryption Mode:** CBC

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 3
Enter the message to be encrypted : introduction to ml
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 2
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 2
The Encrypted Message (cipher_text) is : b'\xf3\xd9\x00\xa1\x11.\xb3\x98\xbe8.j\x9f\xc3\x07;\x1b0\xbf\x03 \xe1\xbc\x97'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 3
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 2
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 2
Enter the cipher_text : b'\xf3\xd9\x00\xa1\x11.\xb3\x98\xbe8.j\x9f\xc3\x07;\x1b0\xbf\x03 \xe1\xbc\x97'
Decrypted Message : itouto omnrdcint l
Decrypted Message (plain_text) : introduction to ml
>>>
Ln: 43 Col: 0

```

- **Encryption Technique:** Transposition Cipher (Simple Transposition)
- **Encryption Algorithm:** 3DES
- **Encryption Mode:** ECB

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 3
Enter the message to be encrypted : introduction to ml
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 3
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 1
The Encrypted Message (cipher_text) is : b'd\x87\xa4\xad\x07 ,\xe8p.c\x19w\xc6V\xb3\x06.\xf5\xd9\x8dZ\xccs'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 3
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 3
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 1
Enter the cipher text : b'd\x87\xa4\xad\x07 ,\xe8p.c\x19w\xc6V\xb3\x06.\xf5\xd9\x8dZ\xccs'
Decrypted Message : itouto omnrdcint l
Decrypted Message (plain_text) : introduction to ml
>>>
Ln: 43 Col: 0

```

- **Encryption Technique:** Transposition Cipher (Simple Transposition)
- **Encryption Algorithm:** 3DES
- **Encryption Mode:** CBC

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 3
Enter the message to be encrypted : computer networks
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 3
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 2
The Encrypted Message (cipher_text) is : b'\xef\x9d\xbbPPu\xf8\x08:\xb6\x02\x19i\xe1N\x14]w\xbex\xba\x00\x97|'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 3
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 3
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 2
Enter the cipher text : b'\xef\x9d\xbbPPu\xf8\x08:\xb6\x02\x19i\xe1N\x14]w\xbex\xba\x00\x97|'
Decrypted Message : cmue ewrsoptrntok
Decrypted Message (plain_text) : computer networks
>>>
Ln: 43 Col: 0

```


- **Encryption Technique:** Transposition Cipher (Double Transposition)
- **Encryption Algorithm:** AES-128
- **Encryption Mode:** ECB

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 4
Enter the message to be encrypted : project management
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 1
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 1
The Encrypted Message (cipher_text) is : b'\xbc\xf4\x05\xdc\x95\xf5\x0e. g\t\xefy:L4\xa4}\xcd%:\x060\xd3\xeeX\x01\x192'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 4
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 1
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 1
Enter the cipher_text : b'\xbc\xf4\x05\xdc\x95\xf5\x0e. g\t\xefy:L4\xa4}\xcd%:\x060\xd3\xeeX\x01\x192'
Decrypted Message : pemgnj aeotnmrcaet
Decrypted Message (plain_text) : project management
>>>
Ln: 16 Col: 7

```

- **Encryption Technique:** Transposition Cipher (Double Transposition)
- **Encryption Algorithm:** AES-128
- **Encryption Mode:** CBC

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 4
Enter the message to be encrypted : project management
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 1
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 2
The Encrypted Message (cipher_text) is : b'*\x92\xe8\xbb\xe5\xa0f\xdb\xefc\x96\xdd\xf6\xc1\xb1\xdG\xf4\x07\r\xc2\xe3t\x0bd\x1e\xdf\xbf\x91\x1dC\x08'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 4
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 1
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 2
Enter the cipher_text : b'*\x92\xe8\xbb\xe5\xa0f\xdb\xefc\x96\xdd\xf6\xc1\xb1\xdG\xf4\x07\r\xc2\xe3t\x0bd\x1e\xdf\xbf\x91\x1dC\x08'
Decrypted Message : pemgnj aeotnmrcaet
Decrypted Message (plain_text) : project management
>>>
Ln: 43 Col: 0

```


- **Encryption Technique:** Transposition Cipher (Double Transposition)
- **Encryption Algorithm:** DES
- **Encryption Mode:** ECB

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 4
Enter the message to be encrypted : artificial intelligence
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 2
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 1
The Encrypted Message (cipher_text) is : b'\x86\xbe\xa4\x10\xe4,\xbf\x9d\x96\xa1\xf4\x19:z\n\xb8v\xc8\xd2\xb0'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 4
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 2
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 1
Enter the cipher_text : b'\x86\xbe\xa4\x10\xe4,\xbf\x9d\x96\xa1\xf4\x19:z\n\xb8v\xc8\xd2\xb0'
Decrypted Message : afanlnriltictc egeiile
Decrypted Message (plain_text) : artificial intelligence
>>>
Ln: 43 Col: 0

```

- **Encryption Technique:** Transposition Cipher (Double Transposition)
- **Encryption Algorithm:** DES
- **Encryption Mode:** CBC

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 4
Enter the message to be encrypted : artificial intelligence
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 2
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 2
The Encrypted Message (cipher_text) is : b'\x8ez\xf3s\x96!\xdc\xad0\x94\xfb\xb5\x82\xc0\xb5r\xa1!T\xbe\x1f\x0b\xe59'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 4
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 2
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 2
Enter the cipher_text : b'\x8ez\xf3s\x96!\xdc\xad0\x94\xfb\xb5\x82\xc0\xb5r\xa1!T\xbe\x1f\x0b\xe59'
Decrypted Message : afanlnriltictc egeiile
Decrypted Message (plain_text) : artificial intelligence
>>>
Ln: 43 Col: 0

```

- **Encryption Technique:** Transposition Cipher (Double Transposition)
- **Encryption Algorithm:** 3DES
- **Encryption Mode:** ECB

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 4
Enter the message to be encrypted : science of programming
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 3
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 1
The Encrypted Message (cipher_text) is : b'z\xcf\xed\x1d\x110\xbec\xc4\x93\xb5\x82v2W\xb99T\xd2\x00[\xb0\xfdK'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 4
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 3
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 1
Enter the cipher_text : b'z\xcf\xed\x1d\x110\xbec\xc4\x93\xb5\x82v2W\xb99T\xd2\x00[\xb0\xfdK'
Decrypted Message : snorane priie gmccfomg
Decrypted Message (plain_text) : science of programming
>>>
Ln: 43 Col: 0

```

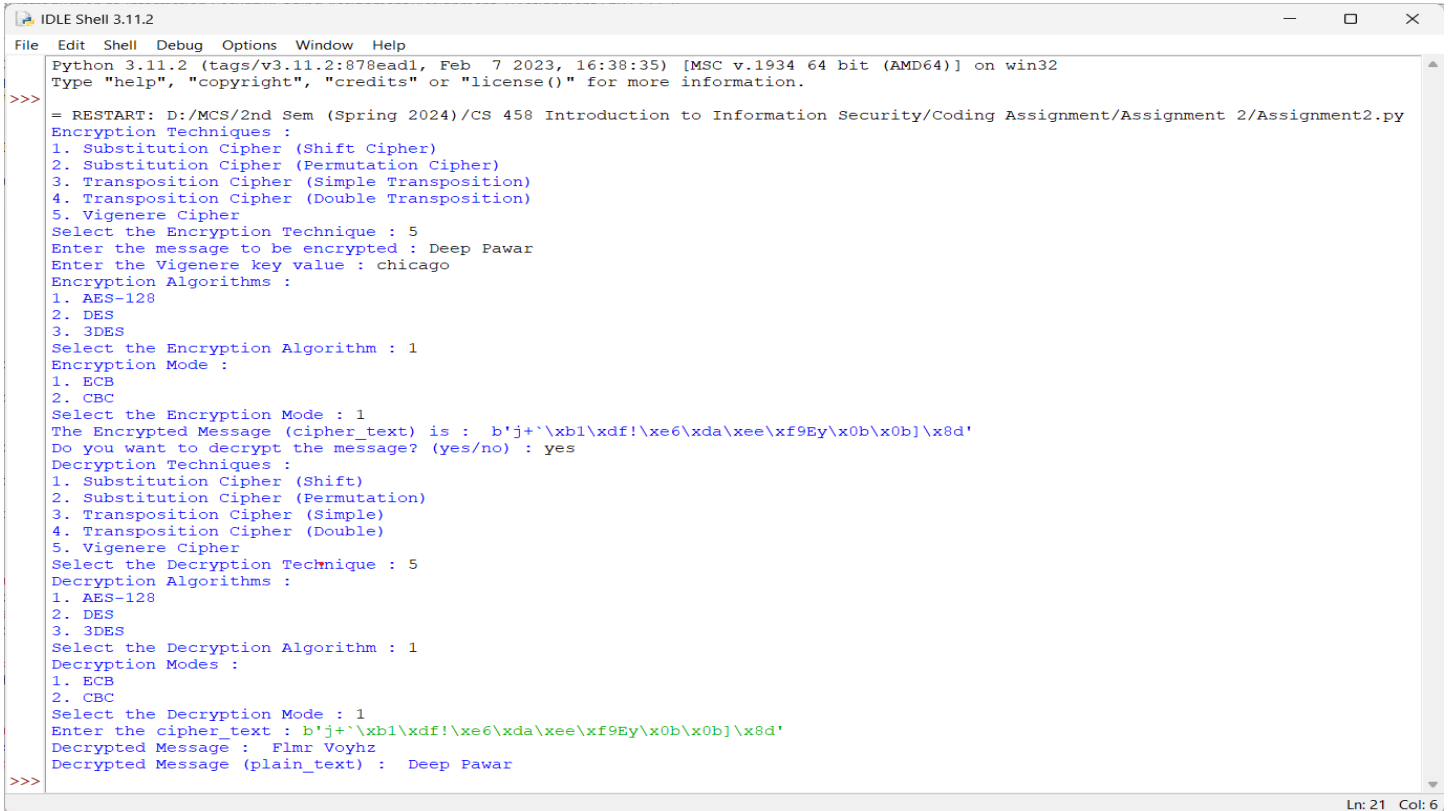
- **Encryption Technique:** Transposition Cipher (Double Transposition)
- **Encryption Algorithm:** 3DES
- **Encryption Mode:** CBC

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 4
Enter the message to be encrypted : science of programming
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 3
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 2
The Encrypted Message (cipher_text) is : b'h\xba\xaa\xd2\x94\xee~\xe0#\xe9\x1a\xdc0\xf4\xbe\xc6\x8e\x84\x14\xa6\x12\xe1\xc7i'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 4
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 3
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 2
Enter the cipher_text : b'h\xba\xaa\xd2\x94\xee~\xe0#\xe9\x1a\xdc0\xf4\xbe\xc6\x8e\x84\x14\xa6\x12\xe1\xc7i'
Decrypted Message : snorane priie gmccfomg
Decrypted Message (plain_text) : science of programming
>>>
Ln: 43 Col: 0

```

- **Encryption Technique:** Vigenere Cipher
- **Encryption Algorithm:** AES-128
- **Encryption Mode:** ECB



```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 5
Enter the message to be encrypted : Deep Pawar
Enter the Vigenere key value : chicago
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 1
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 1
The Encrypted Message (cipher_text) is : b'j+`\\xb1\\xdf!\\xe6\\xda\\xee\\xf9Ey\\x0b\\x0b]\\x8d'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 5
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 1
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 1
Enter the cipher_text : b'j+`\\xb1\\xdf!\\xe6\\xda\\xee\\xf9Ey\\x0b\\x0b]\\x8d'
Decrypted Message : Flmr Voyhz
Decrypted Message (plain_text) : Deep Pawar
>>>
Ln: 21 Col: 6

```

- **Encryption Technique:** Vigenere Cipher
- **Encryption Algorithm:** AES-128
- **Encryption Mode:** CBC



```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 5
Enter the message to be encrypted : deep pawar
Enter the Vigenere key value : chicago
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 1
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 2
The Encrypted Message (cipher_text) is : b'\\xc8\\xe7$\\x98\\xaco`\\`\\`\\xdcY#Icl\\xa3.'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 5
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 1
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 2
Enter the cipher_text : b'\\xc8\\xe7$\\x98\\xaco`\\`\\`\\xdcY#Icl\\xa3.'
Decrypted Message : flmr voyhz
Decrypted Message (plain_text) : deep pawar
>>>
Ln: 3 Col: 0

```

- **Encryption Technique:** Vigenere Cipher
- **Encryption Algorithm:** DES
- **Encryption Mode:** ECB

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 5
Enter the message to be encrypted : lake meadows
Enter the Vigenere key value : south
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 2
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 1
The Encrypted Message (cipher_text) is : b'\xbe\x06[0\x13\x92K1\x07\x82\xdd\x02;\x0b\xfb'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 5
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 2
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 1
Enter the cipher_text : b'\xbe\x06[0\x13\x92K1\x07\x82\xdd\x02;\x0b\xfb'
Decrypted Message : doex esuwvog
Decrypted Message (plain_text) : lake meadows
>>>
Ln: 44 Col: 0

```

- **Encryption Technique:** Vigenere Cipher
- **Encryption Algorithm:** DES
- **Encryption Mode:** CBC

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 5
Enter the message to be encrypted : lake meadows
Enter the Vigenere key value : south
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 2
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 2
The Encrypted Message (cipher_text) is : b'\xc0:\x87L \x9buiU\x04\xdc3uQ\xbbA'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 5
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 2
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 2
Enter the cipher_text : b'\xc0:\x87L \x9buiU\x04\xdc3uQ\xbbA'
Decrypted Message : doex esuwvog
Decrypted Message (plain_text) : lake meadows
>>>
Ln: 44 Col: 0

```

- **Encryption Technique:** Vigenere Cipher
- **Encryption Algorithm:** 3DES
- **Encryption Mode:** ECB

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 5
Enter the message to be encrypted : software architecture
Enter the Vigenere key value : course
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 3
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 1
The Encrypted Message (cipher_text) is : b'\xb2\xc3t{n\x05f\xc3\xc7\xbe\x8c\xf8\xcd\x30\xfb\xef\x11s@\xd0w\x9bt'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 5
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 3
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 1
Enter the cipher_text : b'\xb2\xc3t{n\x05f\xc3\xc7\xbe\x8c\xf8\xcd\x30\xfb\xef\x11s@\xd0w\x9bt'
Decrypted Message : uczkoets rjgjnvwuxwf
Decrypted Message (plain_text) : software architecture
>>>
Ln: 44 Col: 0

```

- **Encryption Technique:** Vigenere Cipher
- **Encryption Algorithm:** 3DES
- **Encryption Mode:** CBC

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/MCS/2nd Sem (Spring 2024)/CS 458 Introduction to Information Security/Coding Assignment/Assignment 2/Assignment2.py
Encryption Techniques :
1. Substitution Cipher (Shift Cipher)
2. Substitution Cipher (Permutation Cipher)
3. Transposition Cipher (Simple Transposition)
4. Transposition Cipher (Double Transposition)
5. Vigenere Cipher
Select the Encryption Technique : 5
Enter the message to be encrypted : software architecture
Enter the Vigenere key value : course
Encryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Encryption Algorithm : 3
Encryption Mode :
1. ECB
2. CBC
Select the Encryption Mode : 2
The Encrypted Message (cipher_text) is : b'\x0c\x02\xb8\x1a\xb9\xb0\x9e\xd3@W\xc52\xa9\xa8Tl&aV\x8f\xec\xec\x02#'
Do you want to decrypt the message? (yes/no) : yes
Decryption Techniques :
1. Substitution Cipher (Shift)
2. Substitution Cipher (Permutation)
3. Transposition Cipher (Simple)
4. Transposition Cipher (Double)
5. Vigenere Cipher
Select the Decryption Technique : 5
Decryption Algorithms :
1. AES-128
2. DES
3. 3DES
Select the Decryption Algorithm : 3
Decryption Modes :
1. ECB
2. CBC
Select the Decryption Mode : 2
Enter the cipher_text : b'\x0c\x02\xb8\x1a\xb9\xb0\x9e\xd3@W\xc52\xa9\xa8Tl&aV\x8f\xec\xec\x02#'
Decrypted Message : uczkoets rjgjnvwuxwf
Decrypted Message (plain_text) : software architecture
>>>
Ln: 44 Col: 0

```