**Coding Assignment 2**

**Report**

**Name:- Pranav Murali**

**CWID:- A20555824**

**Email:-** [**pmurali6@hawk.iit.edu**](mailto:pmurali6@hawk.iit.edu)

The whole code is done in Python and the source code is attached to the file.

1. **Substitution Cipher**

A screenshot of a computer

Description automatically generated

1. **Shift Cipher**

**A black background with a black square

Description automatically generated with medium confidence**

1. **Permutation Cipher**

**A black screen with a black background

Description automatically generated**

1. **Simple Transposition**

**A black screen with white text

Description automatically generated**

1. **Double Transposition**

**A screenshot of a computer

Description automatically generated**

1. **Vigenere Cipher**

**A black screen with a white text

Description automatically generated**

1. **AES Encryption in ECB mode**

**A black screen with white text

Description automatically generated**

1. **AES Encryption in CBC mode**

**A black screen with blue and green text

Description automatically generated**

1. **DES Encryption in ECB mode**

**A black background with yellow lights

Description automatically generated**

1. **DES Encryption in CBC mode**

**A screen shot of a computer

Description automatically generated**

1. **3DES Encryption in ECB mode**

**A black screen with white text

Description automatically generated**

1. **3DES Encryption in CBC mode**

**A black screen with white text

Description automatically generated**

1. **Exit**

**A black background with blue text

Description automatically generated**

1. Substitution Cipher:

The Substitution Cipher involves replacing each letter in the plaintext with another letter based on a predefined mapping or key. For example, 'a' might be replaced with '!', 'b' with '@', and so on. The mapping remains constant throughout the encryption and decryption process.

2. Shift Cipher:

The Shift Cipher, also known as the Caesar Cipher, involves shifting each letter in the plaintext by a fixed number of positions down or up the alphabet. For example, with a shift of 3, 'a' becomes 'd', 'b' becomes 'e', and so on. This shift wraps around the alphabet if necessary.

3. Permutation Cipher:

The Permutation Cipher involves rearranging the characters in the plaintext according to a specific permutation or order. Each character is mapped to a new position based on the permutation. For example, if the permutation is [3, 1, 4, 2], the first character moves to the third position, the second to the first position, and so on.

4. Simple Transposition:

The Simple Transposition Cipher rearranges the characters in the plaintext by writing them into a grid row by row and then reading them out column by column (or vice versa) according to a specific pattern or key. This rearrangement does not change the characters themselves, only their order.

5. Double Transposition:

The Double Transposition Cipher involves applying two successive transpositions to the plaintext. This provides an additional layer of encryption by rearranging the characters twice based on different keys or patterns.

6. Vigenere Cipher:

The Vigenere Cipher is a polyalphabetic substitution cipher that uses a keyword to encrypt the plaintext. Each letter in the keyword corresponds to a shift value, which is used to shift the corresponding letter in the plaintext. The keyword is repeated as necessary to match the length of the plaintext.

7. AES Encryption in ECB mode:

AES (Advanced Encryption Standard) is a symmetric encryption algorithm widely used for securing sensitive data. ECB (Electronic Codebook) mode is a basic mode of operation for block ciphers, where each block of plaintext is encrypted independently with the same key. ECB mode does not use an initialization vector (IV), making it deterministic and potentially vulnerable to certain attacks.

8. AES Encryption in CBC mode:

CBC (Cipher Block Chaining) mode is another mode of operation for block ciphers like AES. In CBC mode, each block of plaintext is XORed with the previous ciphertext block before encryption, adding an element of randomness and making it more secure than ECB mode. CBC mode requires an initialization vector (IV) to start the chaining process.

9. DES Encryption in ECB mode:

DES (Data Encryption Standard) is a symmetric encryption algorithm that operates on blocks of data. In ECB mode, each block of plaintext is encrypted independently with the same key, similar to AES ECB mode. DES uses a 56-bit key and is considered less secure than AES.

10. DES Encryption in CBC mode:

Similar to AES CBC mode, DES CBC mode encrypts plaintext in blocks using the DES algorithm. However, it uses CBC mode of operation, which XORs each plaintext block with the previous ciphertext block before encryption, adding randomness and making it more secure.

11. 3DES Encryption in ECB mode:

Triple DES (3DES) is a variant of DES that applies the DES algorithm three times to each block of plaintext. In ECB mode, it encrypts each block independently with the same triple DES key. 3DES provides stronger security than single DES but is slower and less efficient.

12. 3DES Encryption in CBC mode:

Similar to DES CBC mode, 3DES CBC mode encrypts plaintext using the 3DES algorithm in CBC mode of operation. It provides stronger security than 3DES ECB mode by XORing each plaintext block with the previous ciphertext block before encryption.