Name: Adarsh Mishra
Roll no: 104
Batch: T23

ASSIGNMENT NO 3

Aim: Encrypt long messages using various modes of operation using AES.

Electronic Code Block (ECB)

Theory:

In ECB mode, the plaintext is divided into blocks, and each block is encrypted independently using the same key. This is the simplest mode of operation for block ciphers.

Key Concepts:

- Each block of plaintext is encrypted separately.

- Identical plaintext blocks produce identical ciphertext blocks, which can reveal patterns in the data.

Example:

- Plaintext: ATTACKATDAWN

  - Blocks: ATT, ACK, ATD, AWN

  - Encrypted Blocks: E1, E2, E1, E3 (assuming E1, E2, E3 are the encrypted versions)

Cipher Block Chaining Mode (CBC)

Theory:

In CBC mode, each plaintext block is XORed with the previous ciphertext block before being encrypted. The first plaintext block is XORed with an initialization vector (IV).

Key Concepts:

- Each ciphertext block depends on all previous plaintext blocks.

- Requires an IV for the first block.

- Identical plaintext blocks result in different ciphertext blocks.

Name: Adarsh Mishra
Roll no: 104
Batch: T23

Example:

- Plaintext: ATTACKATDAWN
- Blocks: ATT, ACK, ATD, AWN
- Initialization Vector: IV
- Encrypted Blocks: C1, C2, C3, C4
- C1 = Encrypt(IV XOR ATT)
- C2 = Encrypt(C1 XOR ACK)
- C3 = Encrypt(C2 XOR ATD)
- C4 = Encrypt(C3 XOR AWN)

Output Feedback Mode (OFB)

Theory:

In OFB mode, the encryption of an IV generates a keystream, which is then XORed with the plaintext to produce the ciphertext. This keystream is independent of the plaintext and is generated before encryption.

Key Concepts:

- Converts a block cipher into a stream cipher.
- The keystream depends only on the IV and the key.
- Identical IVs produce identical keystreams.

Example:

- Plaintext: ATTACKATDAWN
- Keystream: KS1, KS2, KS3, KS4 (generated from IV and key)
- Ciphertext: C1, C2, C3, C4
- C1 = KS1 XOR ATT
- C2 = KS2 XOR ACK
- C3 = KS3 XOR ATD
- C4 = KS4 XOR AWN

Name: Adarsh Mishra
Roll no: 104
Batch: T23

Counter Mode (CTR)

Theory:

In CTR mode, a counter is encrypted to produce a keystream block, which is then XORed with the plaintext block to produce the ciphertext. The counter is incremented for each subsequent block.

Key Concepts:

- Converts a block cipher into a stream cipher.
- The counter can be any function that produces a sequence of unique values.
- Parallelizable encryption and decryption.

Example:

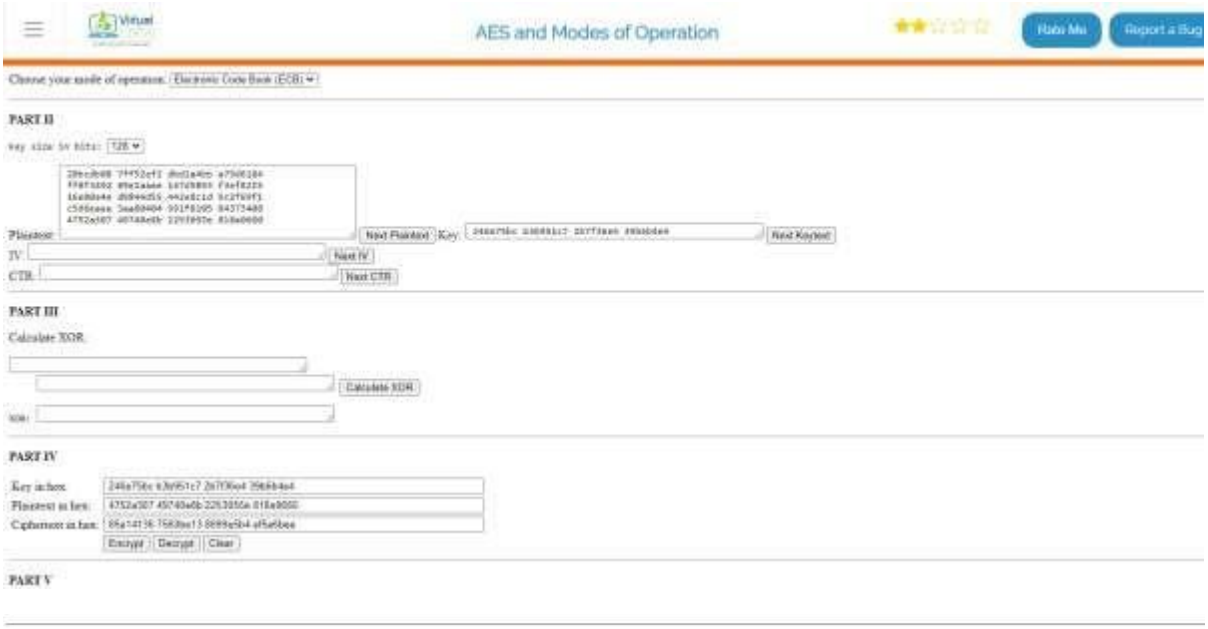
- Plaintext: ATTACKATDAWN
  - Counter: CTR1, CTR2, CTR3, CTR4
  - Keystream: KS1, KS2, KS3, KS4 (generated from encrypting the counter)
  - Ciphertext: C1, C2, C3, C4
    - C1 = KS1 XOR ATT
    - C2 = KS2 XOR ACK
    - C3 = KS3 XOR ATD
    - C4 = KS4 XOR AWN

Each of these modes has its own strengths and weaknesses, and the choice of mode depends on the specific requirements and constraints of the application.

Name: Adarsh Mishra
Roll no: 104
Batch: T23

Screenshots:

Electronic Code Block (ECB)



PART IV

Key in hex: 246e75bc b3b951c7 2b7f36e4 39b6b4e4

Plaintext in hex: 4752a307 49740e8b 2253055e 818a0660

Ciphertext in hex: 85a14136 7560be13 8699e5b4 ef5a6bee

Encrypt | Decrypt | Clear

PART V

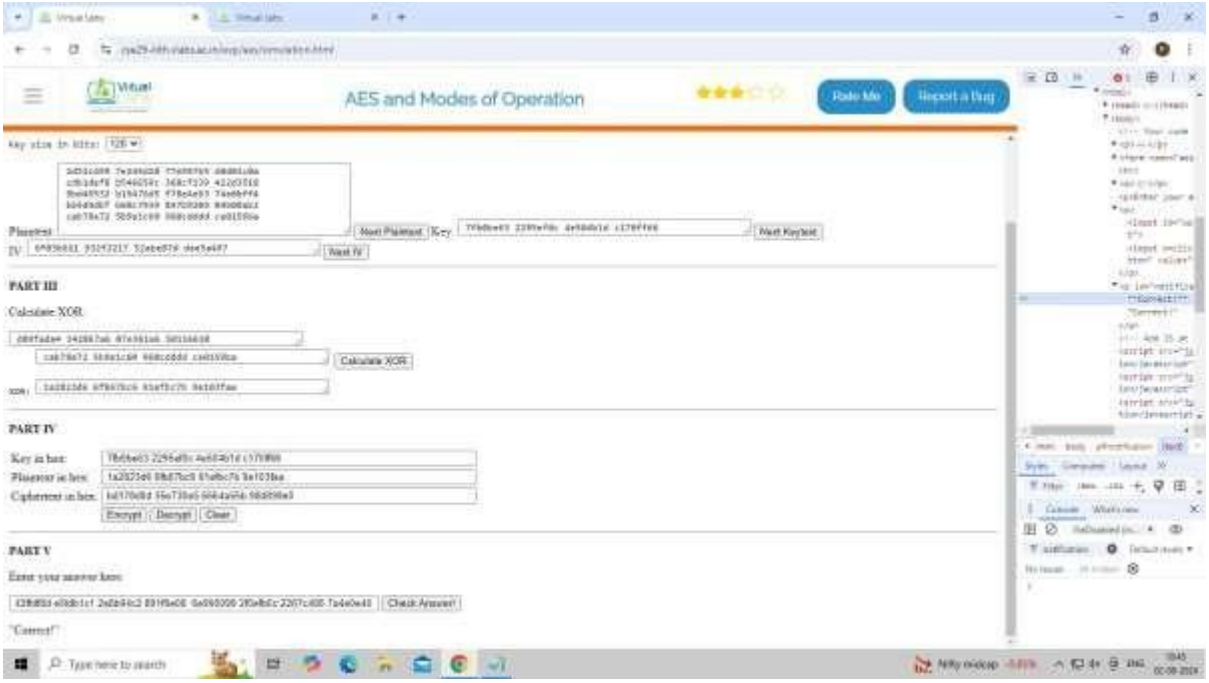
Enter your answer here:

307bacc3 1030633c ddcf908a 13182375 d08966bd 29061711 0dab9034 837f194 | Check Answer!

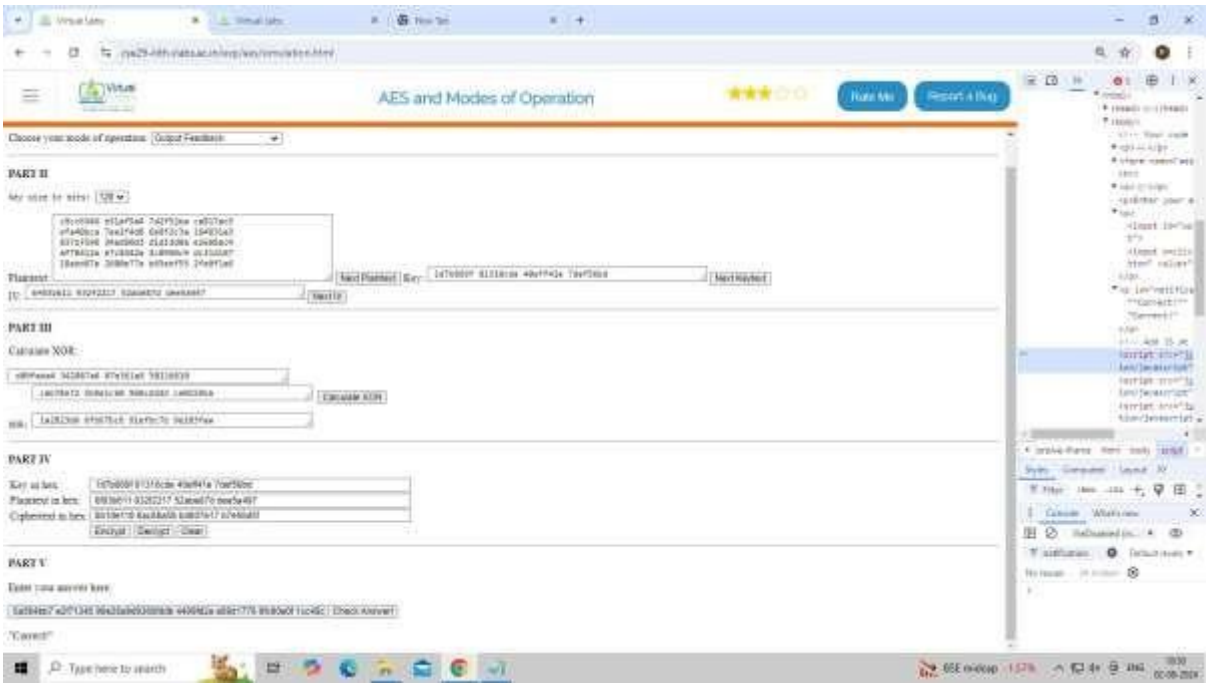
CORRECT!!

Name: Adarsh Mishra
Roll no: 104
Batch: T23

Cipher Block Chaining Mode (CBC)

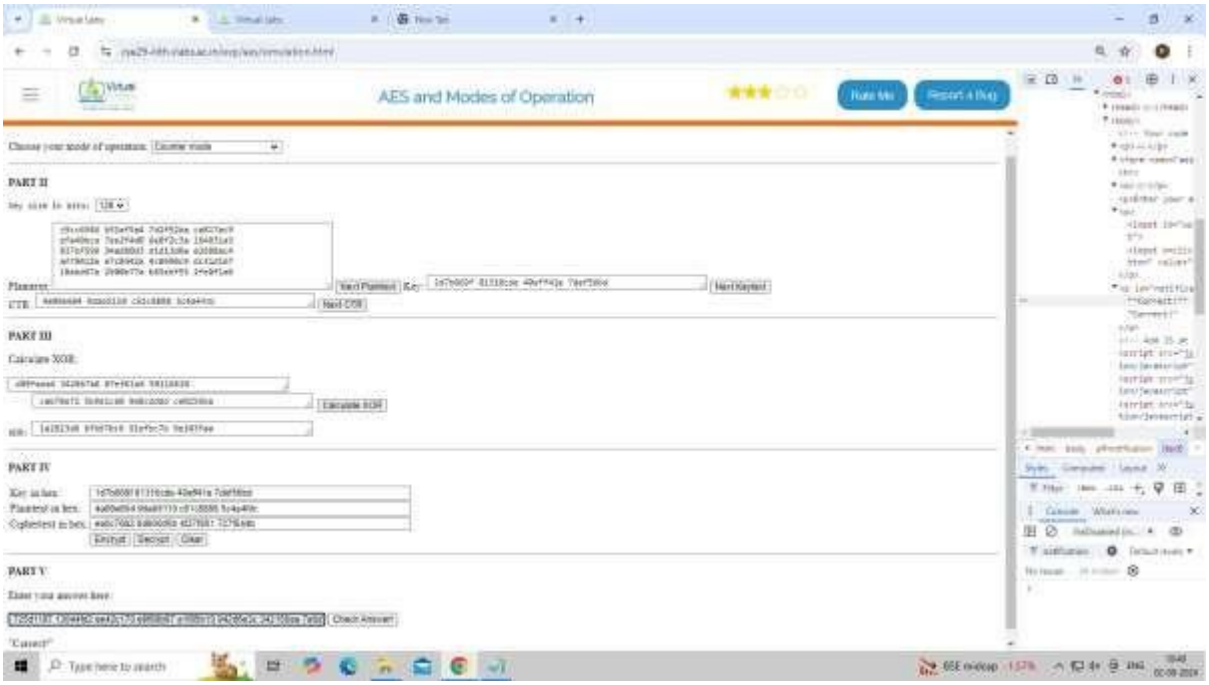


Output Feedback Mode (OFB)



Name: Adarsh Mishra
Roll no: 104
Batch: T23

Counter Mode (CTR)



Conclusion:

In this experiment we learnt about different modes of operations in AES and they are Electronic Code Block, Cipher Block Chaining Mode (CBC) ,Counter Mode (CTR), Output Feedback Mode (OFB). We also learnt to implement them.