Assignment Number: 3

Name: Archie Shah; Branch: I.T (T.E.); Roll Number: 117 25/09/2023

Aim: Block cipher modes of operation using Advanced Encryption Standard (AES).

LO mapped: LO2

Theory:

AES –

The Advanced Encryption Standard (AES) is a widely used symmetric-key encryption algorithm that was established as a federal standard by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is a fundamental component of modern cryptography and is employed in a multitude of applications to secure data transmission and storage. Here's a brief theory about AES:

AES Encryption Algorithm

AES operates on blocks of data and employs a symmetric-key approach, meaning the same key is used for both encryption and decryption. The algorithm accepts plaintext data and transforms it into ciphertext using a series of well-defined steps. These steps involve key expansion, substitution, permutation, and mixing operations. The primary components of AES include:

1. **Key Expansion**: AES supports key sizes of 128, 192, and 256 bits. The key expansion process generates a set of round keys from the original encryption key. These round keys are used in the subsequent rounds of encryption and are derived through a combination of key scheduling and mathematical operations.

2. **Substitution**: AES employs a substitution-permutation network (SPN) structure. In the substitution step, each byte of the plaintext is replaced with a corresponding byte from a fixed substitution table called the S-box. This step introduces confusion and non-linearity into the encryption process.

3. **Permutation**: In this step, the positions of bytes within the block are rearranged. This process, known as mixing or permutation, further enhances the diffusion of data and makes it resistant to attacks.

4. **Mixing**: AES uses a series of matrix multiplication operations called MixColumns. This operation ensures that each byte in the block influences every other byte, providing additional security against various cryptographic attacks.

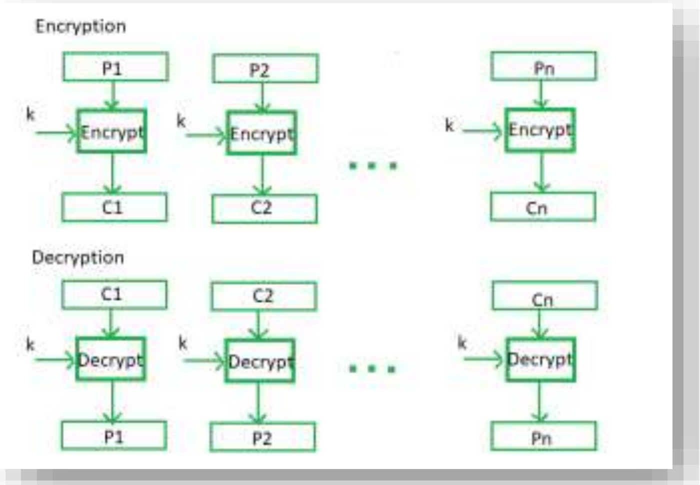
5. **Key Addition**: At the beginning of each round, a round key is XORed (bitwise exclusive OR) with the block of data. This step ensures that each round of encryption is dependent on both the plaintext and the round key.

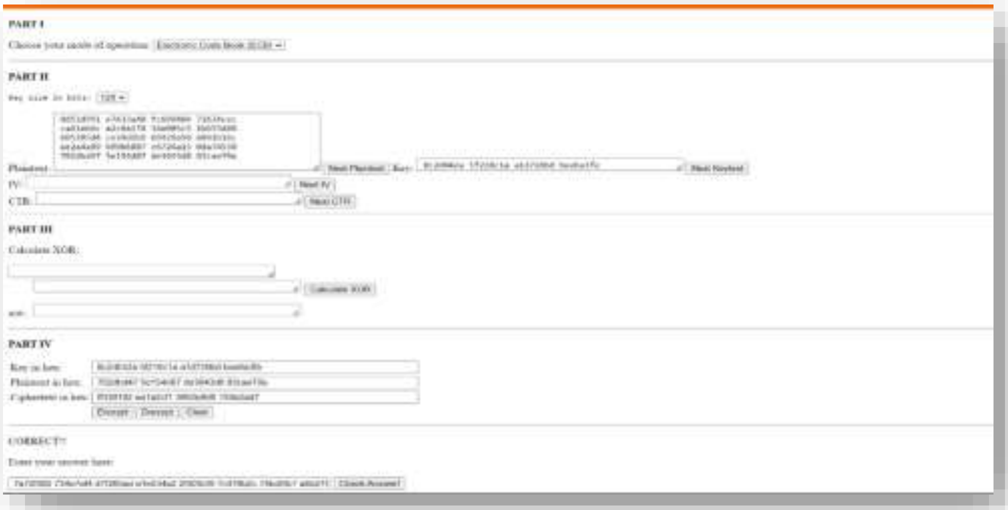
AES Decryption

The decryption process in AES is the reverse of the encryption process. It involves reversing the operations applied during encryption, such as inverse substitution, inverse permutation, and inverse mixing. The round keys are used in reverse order during decryption.

In AES (Advanced Encryption Standard), there are several modes of operation that dictate how the encryption algorithm is applied to plaintext data to produce ciphertext. These modes determine how blocks of data are processed and how they relate to each other. Here's an explanation of some common modes of operation in AES:

1. **Electronic Codebook (ECB)**:
    - **Description**: In ECB mode, each block of plaintext is encrypted independently with the same encryption key. This means that identical blocks of plaintext will result in identical blocks of ciphertext.





PART I

Choose your mode of operation: Electronic Code Book (ECB)

PART II

Key size in bits: 128

Plaintext: [illegible] Next Plaintext Key: [illegible] Next Keytext

IV: Next IV

CTR: Next CTR

PART III

Calculate XOR:

Calculate XOR

xor:

PART IV

Key in here: [illegible]

Plaintext in here: [illegible]

Ciphertext in here: [illegible]

Encrypt Decrypt Clear

CORRECT!!

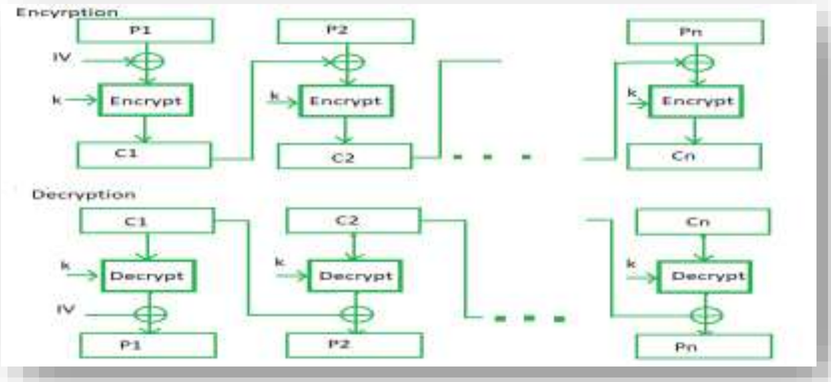
Enter your answer here:

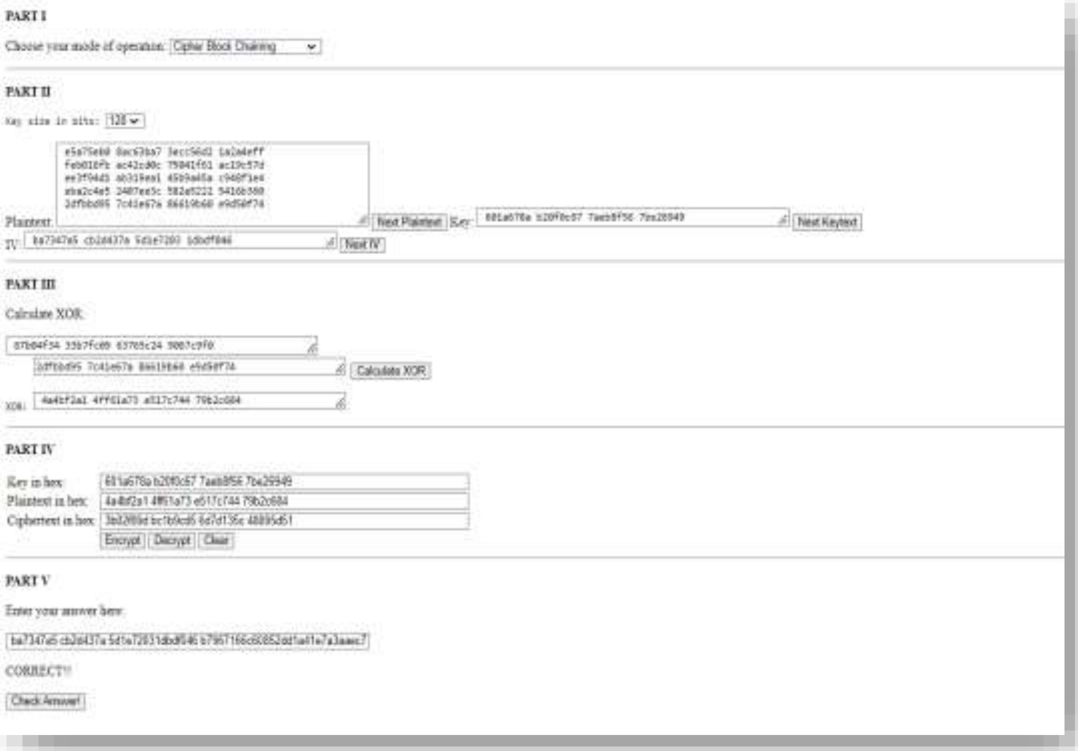
[illegible] Check Answer!

- **Advantages**: Simple and parallelizable, making it suitable for hardware implementation.
- **Drawbacks**: Lack of diffusion (repetitive patterns in plaintext produce repetitive patterns in ciphertext), and it's not suitable for encrypting large amounts of data with the same key.

2. **Cipher Block Chaining (CBC)**:

- **Description**: In CBC mode, each plaintext block is XORed with the ciphertext of the previous block before encryption. The initialization vector (IV) is XORed with the first plaintext block to add randomness to the process.





PART I

Choose your mode of operation: Cipher Block Chaining

PART II

Key size in bits: 128

Plaintext:

```
e5a75e80 8ac63ba7 3ecc56d2 1a2a4eff
feb010fb ac42cd0c 75041f61 ac19c57d
ee3f94d3 ab319ea1 45b9a45a c940f1e4
eba2c4e5 2407ee5c 582e5222 5416b380
3dfbbd95 7c41e67a 86619b60 e9d50f74
```

Key: 681a678a b20f0c67 7aeb8f56 7ba29949

IV: ba7347a5 cb2d437a 5d1e7283 1dbdf846

PART III

Calculate XOR:

77b04f34 33b7fc09 63765c24 9067c9f0

3dfbbd95 7c41e67a 86619b60 e9d50f74

XOR: 4a4bf2a1 4ff61a73 e517c744 79b2c684

PART IV

Key in hex: 681a678a b20f0c67 7aeb8f56 7ba29949

Plaintext in hex: 4a4bf2a1 4ff61a73 e517c744 79b2c684

Ciphertext in hex: 3b82f89d bc1b9cd6 6d7d135c 48895d51

PART V

Enter your answer here:

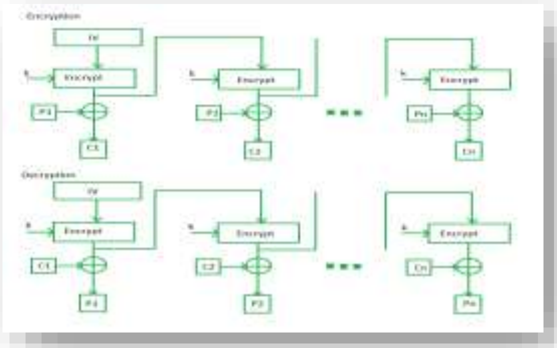
ba7347a5cb2d437a5d1e72831dbdf846b7967166c60852dd1a41e7a3aaec7

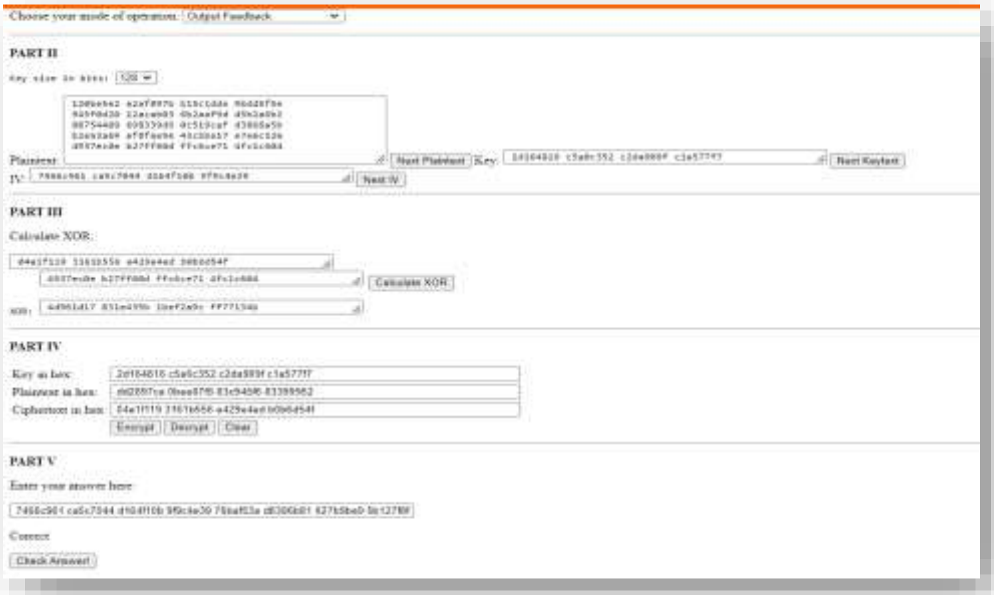
CORRECT!!

- **Advantages**: Provides better security than ECB as it eliminates identical ciphertext blocks, and it can be used for encrypting large files.
- **Drawbacks**: Not parallelizable due to the sequential nature of block chaining, and it requires an IV.

3. **Output Feedback (OFB)**:

- **Description**: OFB mode turns AES into a synchronous stream cipher. It encrypts an IV to produce a keystream, which is XORed with the plaintext to produce ciphertext. It does not depend on the plaintext.





Choose your mode of operation: Output Feedback

PART II

Key size in bits: 128

Plaintext:

```
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
```

Key: 2d164816 c5a6c352 c2da989f c1a57747

IV: 7466c961 ca5c7044 d1d4f10b 9f9c4e39

PART III

Calculate XOR:

d4e1f119 31610556 e429e4ed b0b6d54f

d5f7ed8e b27ff08d ffcbce71 dfc1c084

XOR: 4d961d17 831e4956 1bef2a9c ff77154b

PART IV

Key in hex: 2d164816 c5a6c352 c2da989f c1a577f7

Plaintext in hex: d4d2887ca 0bea87f6 83c94586 83399962

Ciphertext in hex: f4e1f119 3161b656 e429e4ed b0b6d54f

PART V

Enter your answer here:

7466c961 ca5c7044 d1d4f10b 9f9c4e39 78baf63a c8306b81 427b5be0 9e127f8f

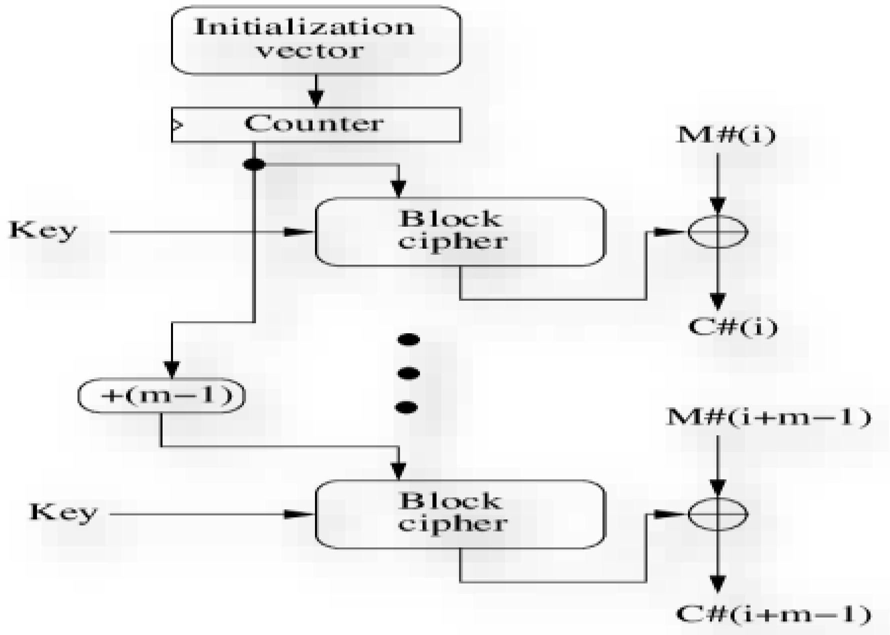
Correct

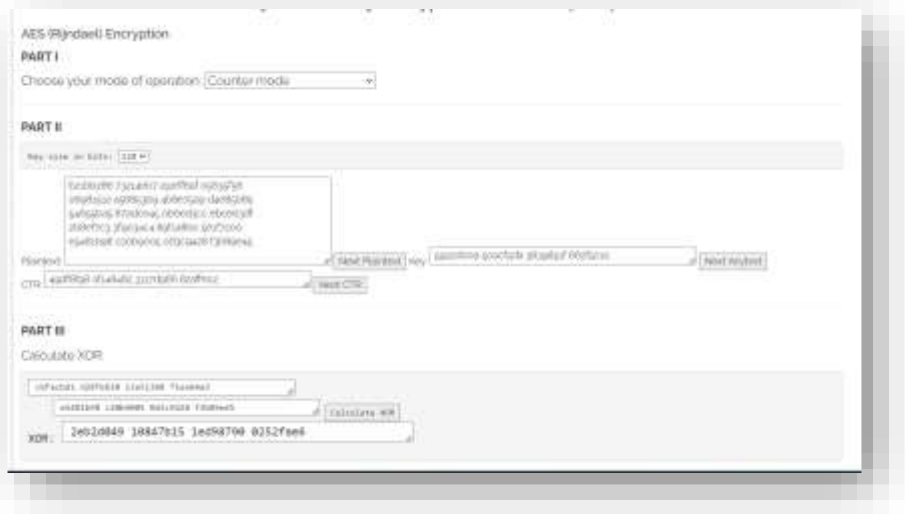
- **Advantages**: Parallelizable and suitable for encrypting data of varying lengths.

- **Drawbacks**: Error propagation (a single bit error affects the entire block), and it requires synchronization between sender and receiver.

4. **Counter (CTR)**:

- **Description**: CTR mode transforms AES into a stream cipher by encrypting a counter value (incremented for each block) to generate a keystream. The keystream is then XORed with the plaintext.





AES (Rijndael) Encryption

PART I

Choose your mode of operation: Counter mode

PART II

Key size in bits: 128

Plaintext: [illegible]

Key: [illegible]

CTR: [illegible]

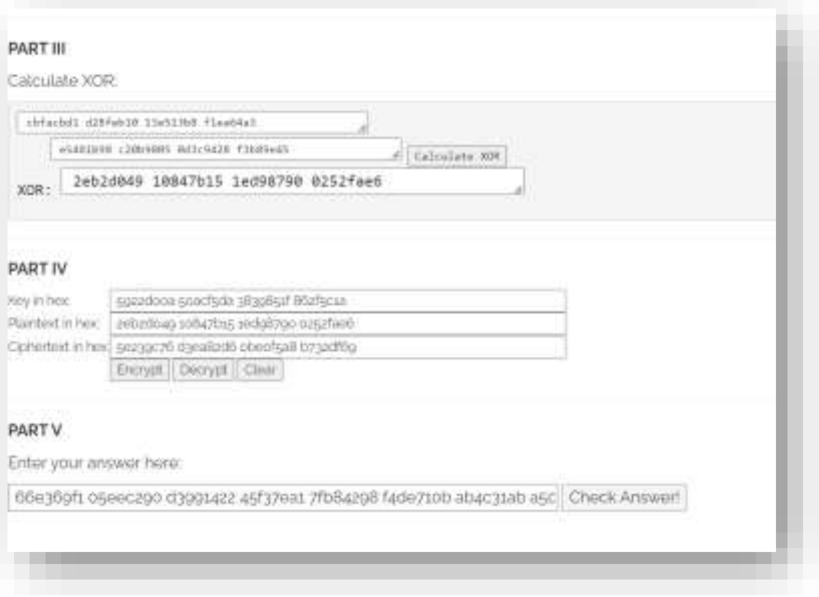
PART III

Calculate XOR:

[illegible]

[illegible]

XOR: 2eb2d049 10847b15 1ed98790 0252fae6



PART III

Calculate XOR:

cbfacbd1 d28feb10 13e513b8 f1ea64a3

e5481b98 c20b9805 8d3c9428 f3b89ed5

XOR: 2eb2d049 10847b15 1ed98790 0252fae6

PART IV

Key in hex: 5922d00a 510cf5da 3830851f 862f5c1a

Plaintext in hex: 2eb2d049 10847b15 1ed98790 0252fae6

Ciphertext in hex: 5e239c76 d3ea82d6 0be0f5a8 b732df69

PART V

Enter your answer here:

66e369f1 05eec290 d3991422 45f37ea1 7fb84298 f4de710b ab4c31ab a5c

- **Advantages**: Highly parallelizable, efficient for random access to data, and provides good security.
- **Drawbacks**: Requires a unique counter for each plaintext block to avoid security issues.

Conclusion: By this assignment we learned various modes of operation of AES algorithm.