Assignment Number: 3

Name: Deep Prajapati ; Branch: I.T (T.E.); Roll Number: 96 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.

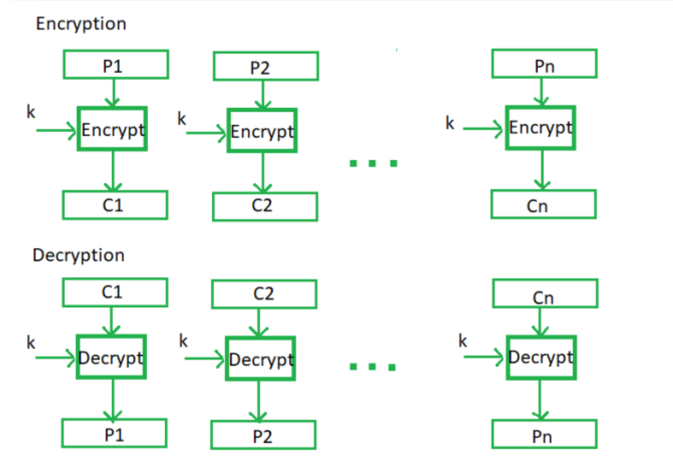
5. **Key Addition**: At the beginning of each round, a round key is XORed (bitwise exclusive OR) with the block of data. This step ensures that each round of encryption is dependent on both the plaintext and the round key.

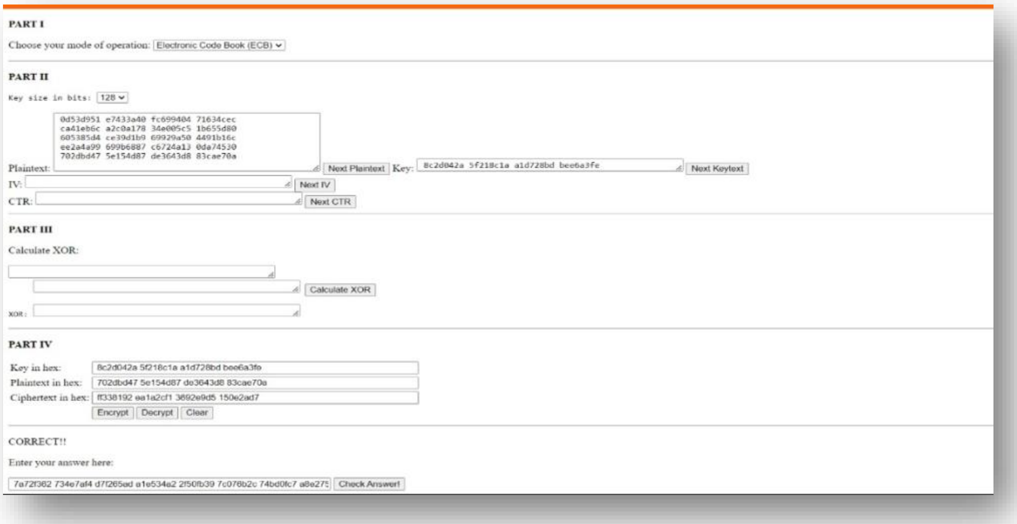
AES Decryption

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

```
0d53d951 e7433a40 fc699404 71634cec
ca41eb6c a2c0a178 34e005c5 1b655d80
605385d4 ce39d1b9 69929a50 4491b16c
ee2a4a99 699b6887 c6724a13 0da74530
702dbd47 5e154d87 de3643d8 83cae70a
```

Plaintext: Key: 8c2d042a 5f218c1a a1d728bd bee6a3fe

IV:

CTR:

PART III

Calculate XOR:

XOR :

PART IV

Key in hex: 8c2d042a 5f218c1a a1d728bd bee6a3fe

Plaintext in hex: 702dbd47 5e154d87 de3643d8 83cae70a

Ciphertext in hex: ff338192 ea1a2cf1 3692e9d5 150e2ad7

CORRECT!!

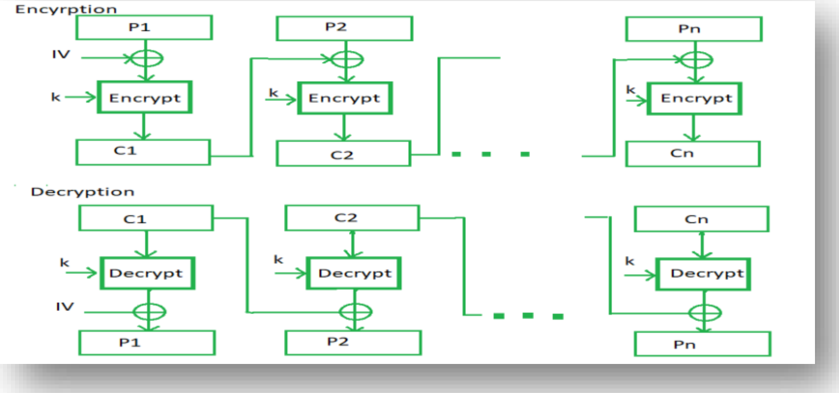
Enter your answer here:

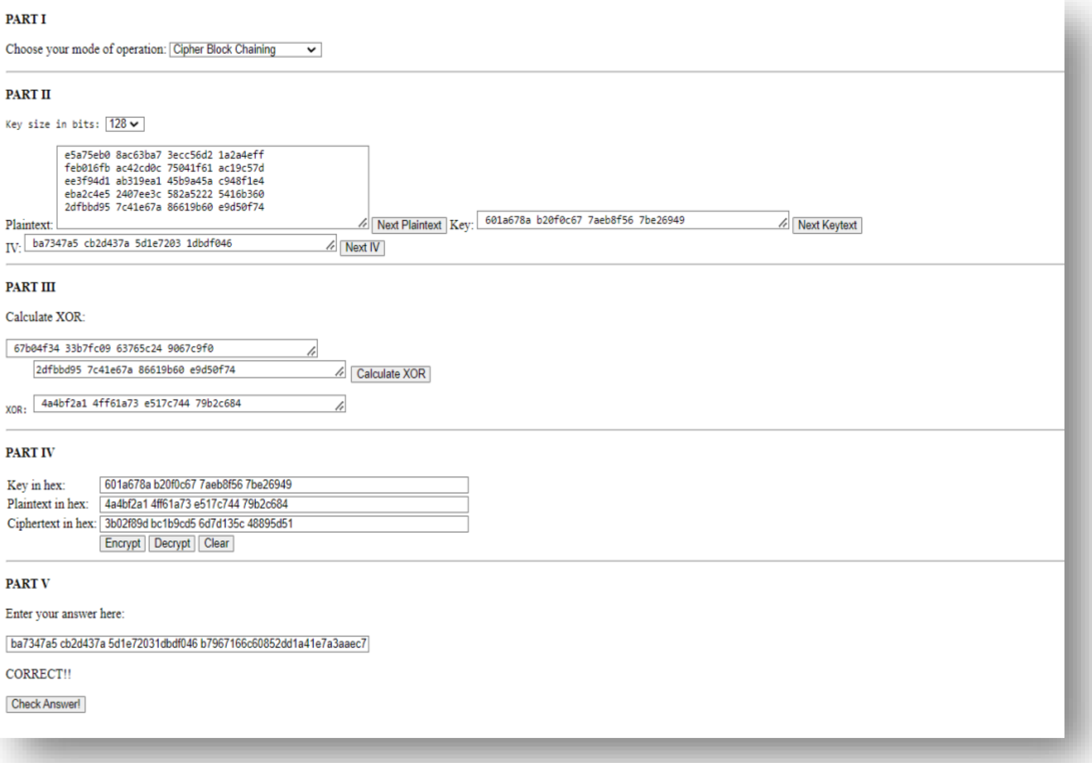
7a72f362 734e7af4 d7f265ad a1e534a2 2f50fb39 7c076b2c 74bd0fc7 a8e275

- **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:
```
e5a75eb0 8ac63ba7 3ecc56d2 1a2a4eff
feb016fb ac42cd0c 75041f61 ac19c57d
ee3f94d1 ab319ea1 45b9a45a c948f1e4
eba2c4e5 2407ee3c 582a5222 5416b360
2dfbbd95 7c41e67a 86619b60 e9d50f74
```

Key: 601a678a b20f0c67 7aeb8f56 7be26949

IV: ba7347a5 cb2d437a 5d1e7203 1dbdf046

PART III

Calculate XOR:

67b04f34 33b7fc09 63765c24 9067c9f0

2dfbbd95 7c41e67a 86619b60 e9d50f74

XOR: 4a4bf2a1 4ff61a73 e517c744 79b2c684

PART IV

Key in hex: 601a678a b20f0c67 7aeb8f56 7be26949

Plaintext in hex: 4a4bf2a1 4ff61a73 e517c744 79b2c684

Ciphertext in hex: 3b02f89d bc1b9cd5 6d7d135c 48895d51

PART V

Enter your answer here:

ba7347a5 cb2d437a 5d1e72031dbdf046 b7967166c60852dd1a41e7a3aaec7

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.

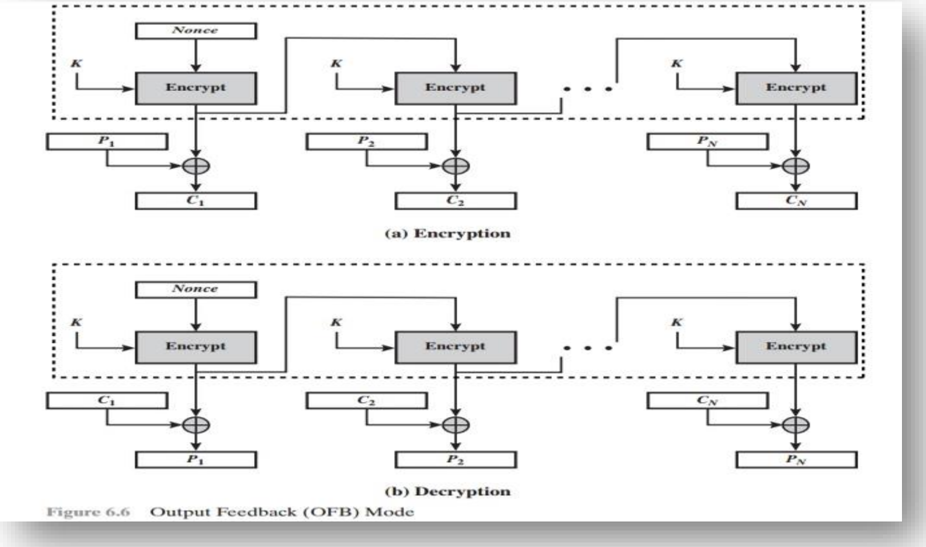
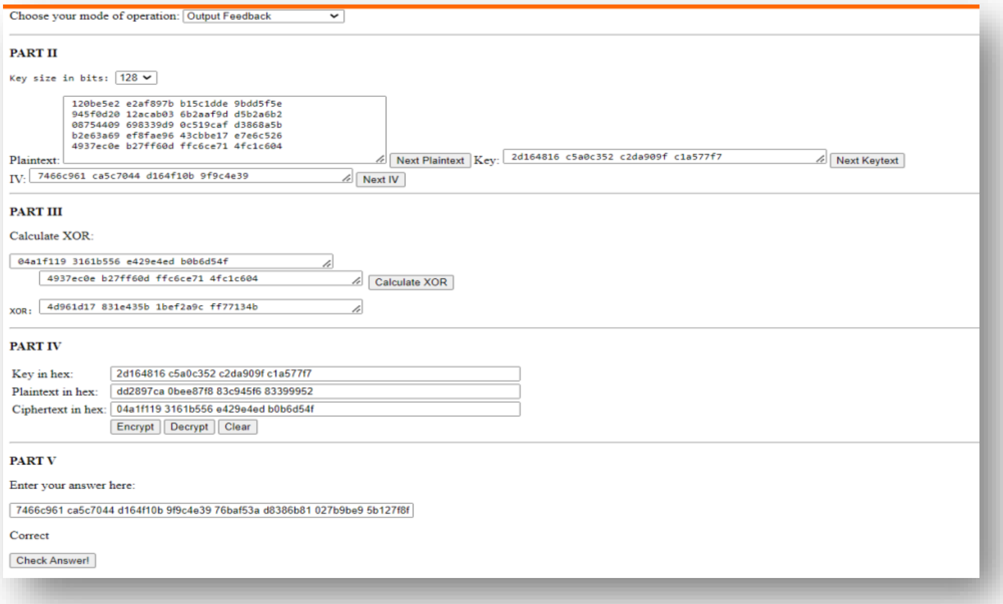


Figure 6.6 Output Feedback (OFB) Mode



Choose your mode of operation: Output Feedback

PART II

Key size in bits: 128

```
120be5e2 e2af897b b15c1dde 9bdd5f5e
945f0d20 12acab03 6b2aaf9d d5b2a6b2
08754409 698339d9 0c519caf d3868a5b
b2e63a69 ef8fae96 43cbbe17 e7e6c526
4937ec0e b27ff60d ffc6ce71 4fc1c604
```

Plaintext: Key: 2d164816 c5a0c352 c2da909f c1a577f7

IV: 7466c961 ca5c7044 d164f10b 9f9c4e39

PART III

Calculate XOR:

04a1f119 3161b556 e429e4ed b0b6d54f

4937ec0e b27ff60d ffc6ce71 4fc1c604

XOR: 4d961d17 831e435b 1bef2a9c ff77134b

PART IV

Key in hex: 2d164816 c5a0c352 c2da909f c1a577f7

Plaintext in hex: dd2897ca 0bee87f8 83c945f6 83399952

Ciphertext in hex: 04a1f119 3161b556 e429e4ed b0b6d54f

PART V

Enter your answer here:

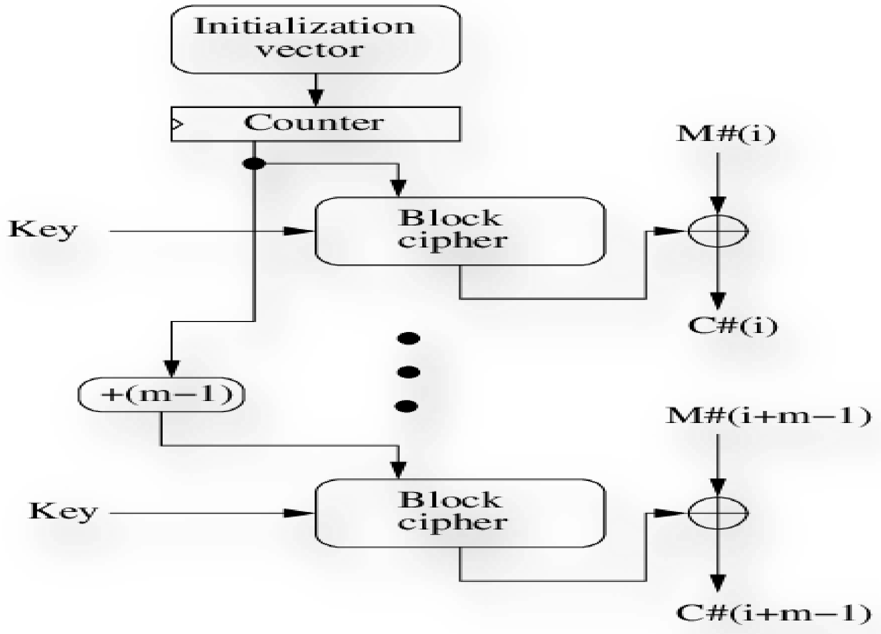
7466c961 ca5c7044 d164f10b 9f9c4e39 76baf53a d8386b81 027b9be9 5b127f8f

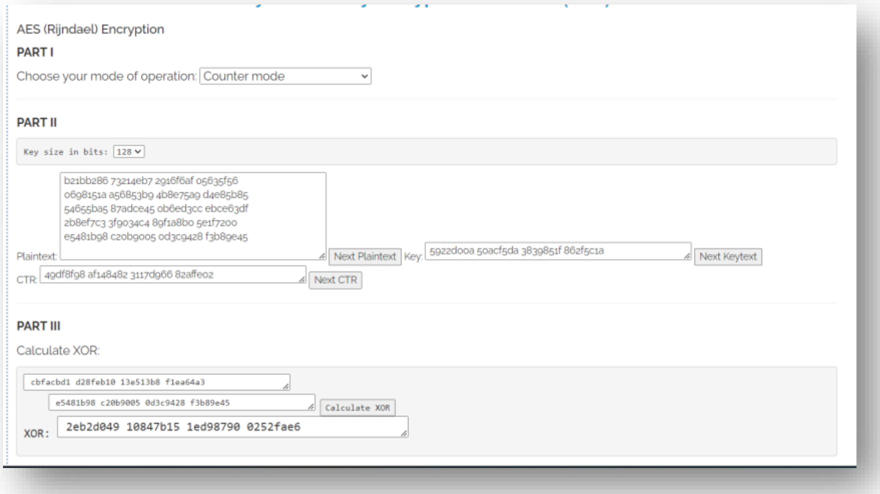
Correct

- **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:
```
b21bb286 73214eb7 2916f6af 05635f56
0698151a a56853b9 4b8e75a9 d4e85b85
54655ba5 87adce45 0b6ed3cc ebce63df
2b8ef7c3 3f9034c4 89f1a8b0 5e1f7200
e5481b98 c20b9005 0d3c9428 f3b89e45
```

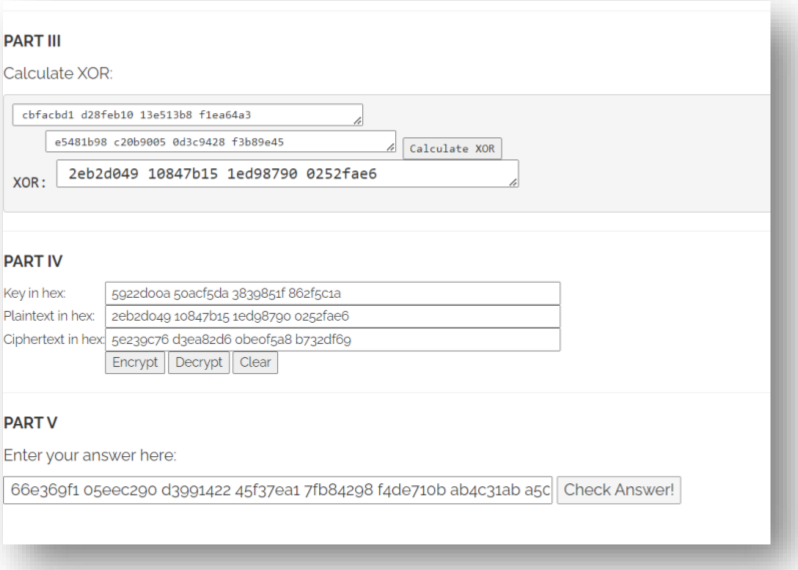
Key: 5922d00a 50acf5da 3839851f 862f5c1a

CTR: 49df8f98 af148482 3117d966 82affe02

PART III

Calculate XOR:

```
cbfacbd1 d28feb10 13e513b8 f1ea64a3
e5481b98 c20b9005 0d3c9428 f3b89e45
XOR: 2eb2d049 10847b15 1ed98790 0252fae6
```



PART III

Calculate XOR:

```
cbfacbd1 d28feb10 13e513b8 f1ea64a3
e5481b98 c20b9005 0d3c9428 f3b89e45
XOR: 2eb2d049 10847b15 1ed98790 0252fae6
```

PART IV

Key in hex: 5922d00a 50acf5da 3839851f 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.