Experiment No 3

Aim : Block Cipher modes of operations using Advanced Encryption Techniques.

Lab Outcome :

LO2

Theory :

1. AES Algorithm?

The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm known for its security and efficiency. AES is a block cipher, which means it operates on fixedsize blocks of data and applies a series of transformations to encrypt or decrypt the data. It was adopted by the U.S. government as a standard encryption algorithm in 2001 and has since become a fundamental component of modern cryptography.

Cipher Type:

AES is a symmetric key cipher, also known as a secret-key or private-key cipher. This means that the same secret key is used for both encryption and decryption. The security of AES relies on the strength of the secret key, making it essential to keep the key secret and protected.

Number of Rounds:

AES operates in multiple rounds of transformations to ensure strong security. The number of rounds varies based on the key size:

- For AES-128: 10 rounds

- For AES-192: 12 rounds - For AES-256: 14 rounds

Key Size:

AES supports three different key sizes: 128 bits, 192 bits, and 256 bits. The key size directly affects the algorithm's security, with larger key sizes generally providing higher levels of security.

Block Size:

AES has a fixed block size of 128 bits (16 bytes). This means that the input plaintext is divided into blocks of 128 bits each for encryption or decryption.

Operations in Each Round:

Each round of AES consists of several cryptographic operations, including SubBytes, ShiftRows, MixColumns, and AddRoundKey. Here's a brief overview of these operations:

1. SubBytes:

In this operation, each byte of the input block is replaced by a corresponding byte from a fixed substitution table called the S-box. The S-box is designed to introduce confusion in the data and provide non-linearity to the encryption process.

2. ShiftRows:

In this step, the rows of the block are shifted by varying numbers of bytes. The first row is not shifted, the second row is shifted by one byte to the left, the third row by two bytes, and the fourth row by three bytes. This operation ensures that the data is spread out in a way that contributes to the diffusion property of encryption.

3. MixColumns:

This step operates on the columns of the block, treating each column as a four-term polynomial. MixColumns uses matrix multiplication operations to mix the bytes within each column. This operation further enhances the encryption's diffusion and confusion properties.

4. AddRoundKey:

A round key is generated from the main encryption key for each round. In the AddRoundKey step, each byte of the block is bitwise XORed with the corresponding byte of the round key. This step ensures that the input data is mixed with the current round's key, providing additional security.

After completing the specified number of rounds, the AES encryption process is complete. Decryption involves applying the inverse of each operation in reverse order using the same round keys.

AES's combination of substitution, permutation, diffusion, and confusion operations, along with the varying number of rounds based on key size, contributes to its robust security and widespread adoption in secure communication, data storage, and various cryptographic applications.

2. With diagram explain in brief block cipher modes of operation:

ECB mode

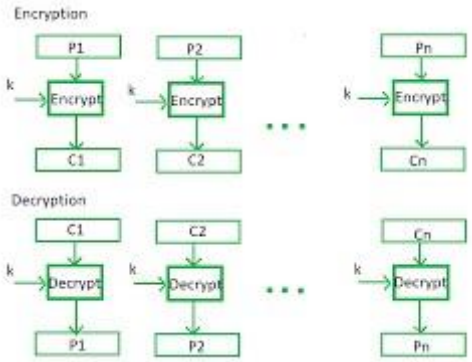
CBC mode

OFB mode

Counter mode

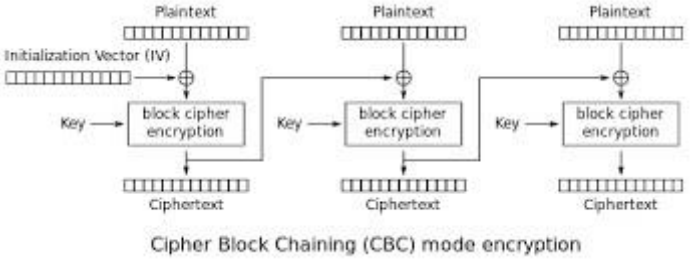
Block cipher modes of operation are techniques used to apply a block cipher, which is a cryptographic algorithm that encrypts fixed-size blocks of data, to larger amounts of data. These modes determine how blocks of plaintext are encrypted and how the resulting ciphertext is generated. Let's explore four common block cipher modes of operation: ECB, CBC, OFB, and Counter mode, along with a brief explanation and diagrams for each.

1. ECB (Electronic Codebook) Mode:
ECB mode is the simplest block cipher mode. It encrypts each block of plaintext independently using the same key, resulting in a corresponding block of ciphertext. While simple, ECB has some weaknesses. Identical plaintext blocks will produce identical ciphertext blocks, which can leak information, and it doesn't provide semantic security.



2. CBC (Cipher Block Chaining) Mode:

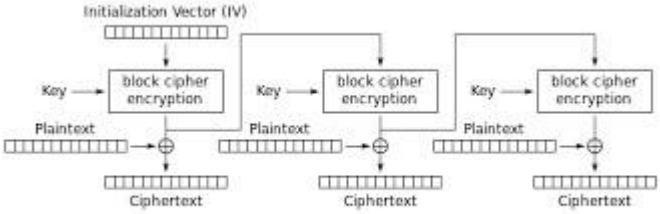
CBC mode addresses the weaknesses of ECB mode by introducing an Initialization Vector (IV) and chaining blocks together. Each plaintext block is XORed with the previous ciphertext block (or the IV for the first block), and then encrypted. This chaining introduces randomness and prevents identical blocks from producing identical ciphertext blocks. CBC is widely used and offers better security.



Cipher Block Chaining (CBC) mode encryption

3. OFB (Output Feedback) Mode:

OFB mode transforms the block cipher into a stream cipher by generating a keystream of random data blocks using the encryption process. This keystream is then XORed with the plaintext to produce the ciphertext. The advantage of OFB is that errors in ciphertext transmission do not propagate, as they would in CBC. However, it doesn't offer integrity checking or error detection.



Output Feedback (OFB) mode encryption

4. Counter Mode:

Counter mode turns a block cipher into a stream cipher by using a counter to generate a sequence of unique values. Each counter value is encrypted with the key to produce a keystream, which is then XORed with the plaintext to create the ciphertext. Counter mode is highly parallelizable and can be more efficient than other modes. It's also suitable for applications like disk encryption and random number generation.

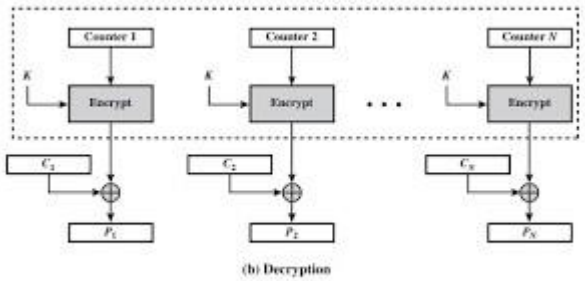
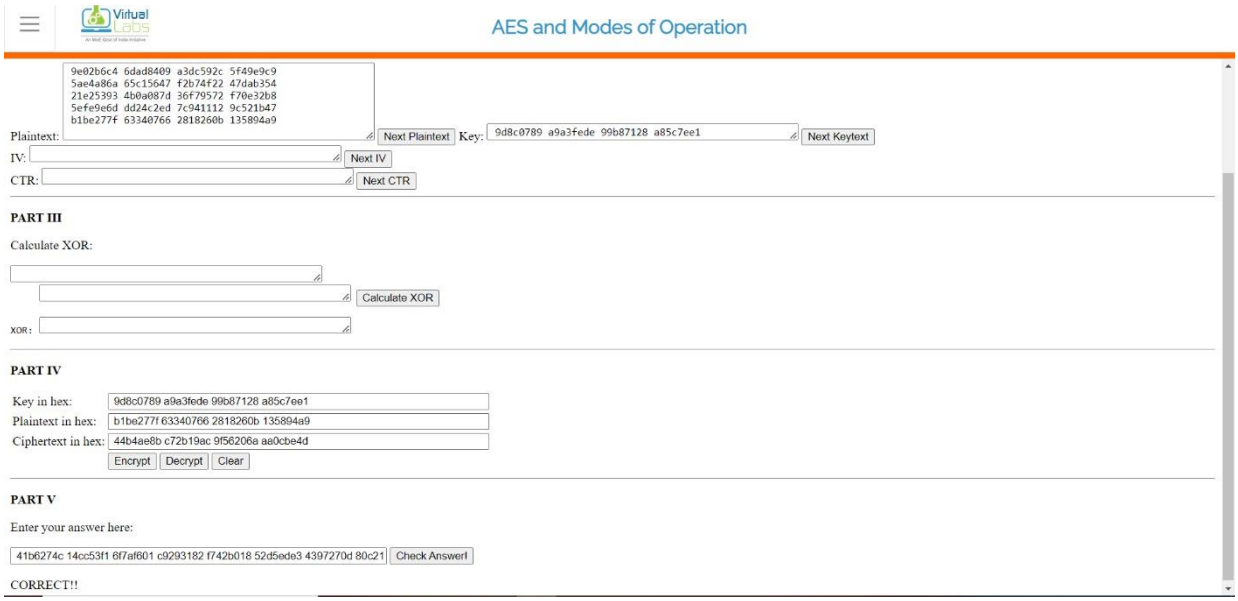
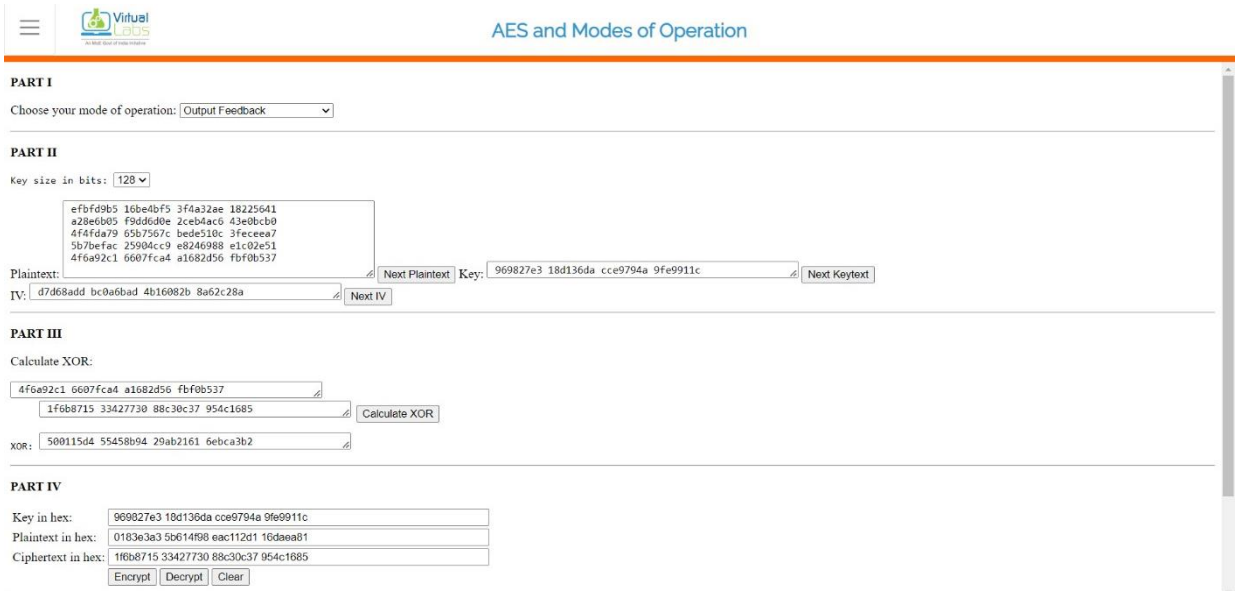


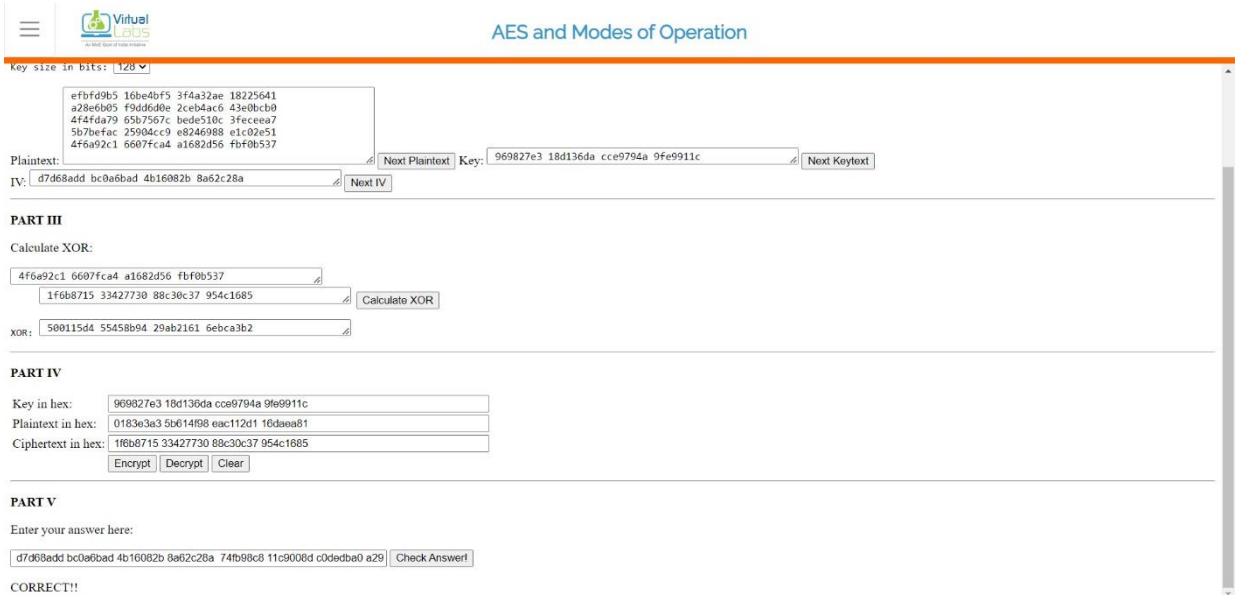
Figure 6.7 Counter (CTR) Mode

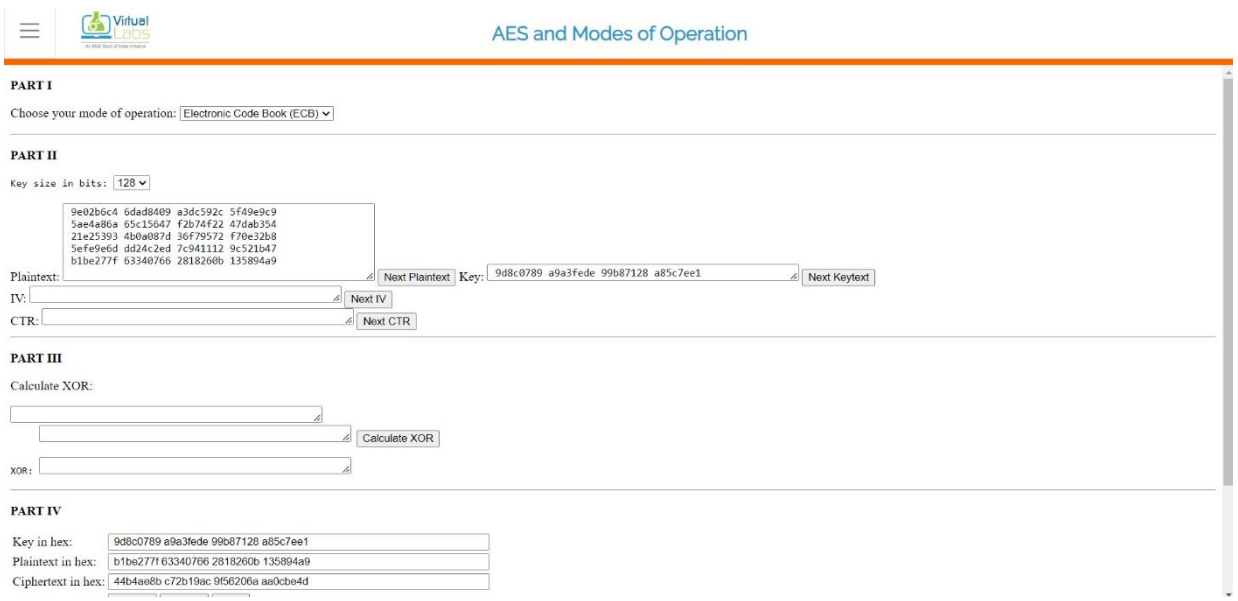
Block cipher modes of operation play a crucial role in making block ciphers practical for encrypting larger amounts of data. Each mode has its strengths and weaknesses, and the choice of mode depends on the specific requirements of the application. It's important to choose the appropriate mode based on factors such as security, performance, and desired features like error propagation or parallelizability. Always ensure you're using a well-established and properly implemented cryptographic library or tool to achieve secure data encryption.

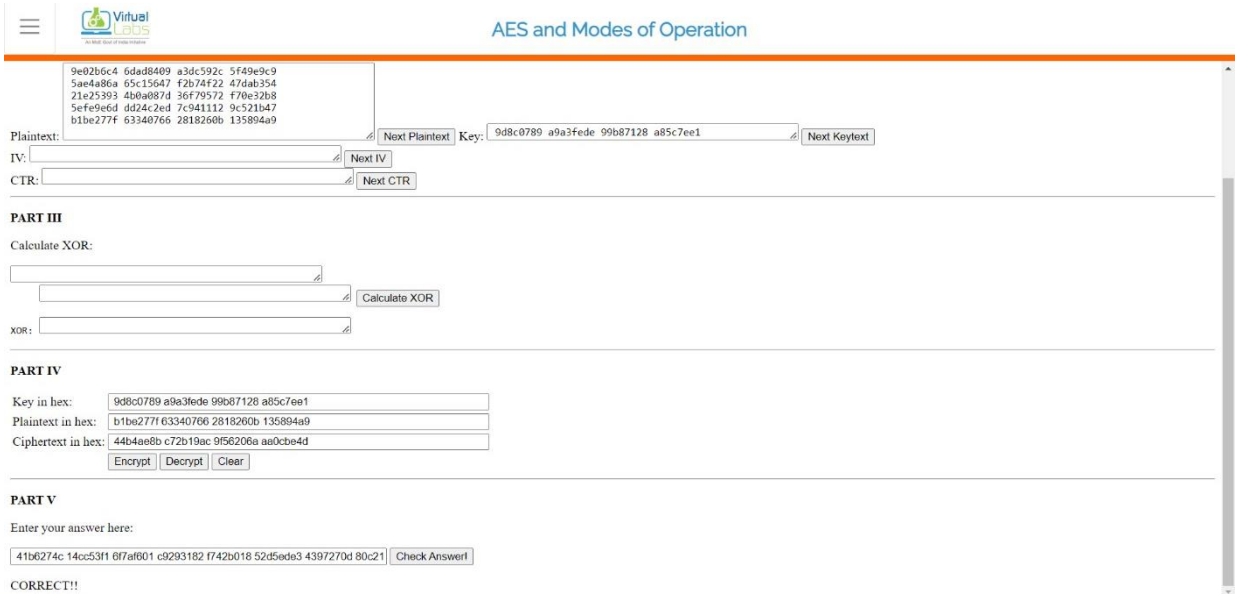
Output:

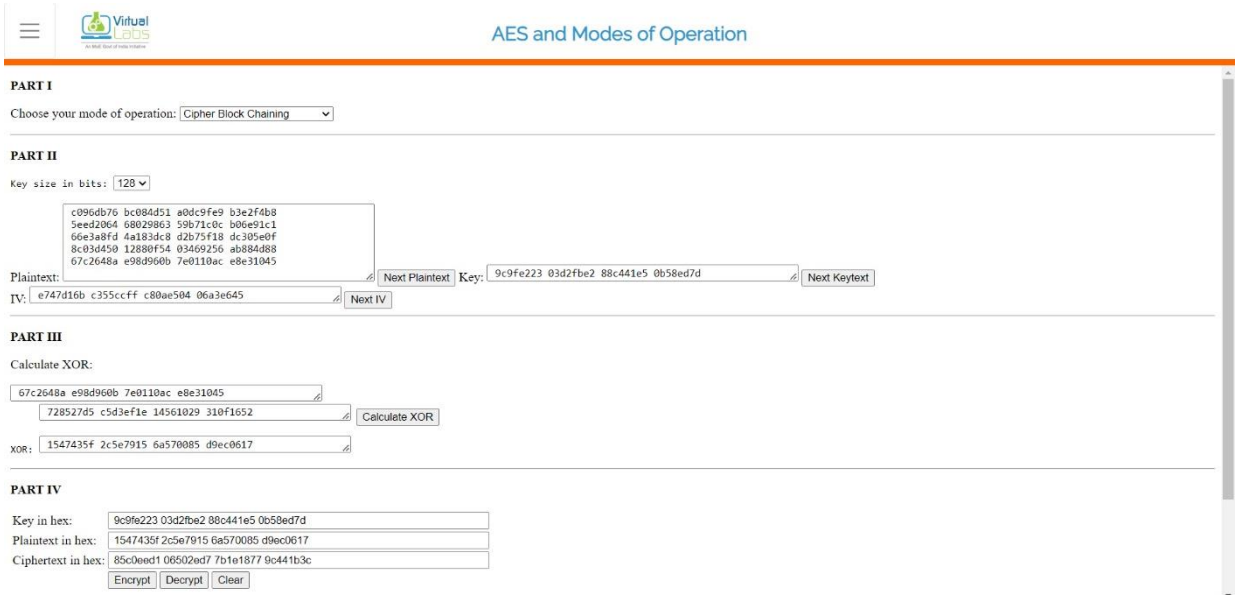


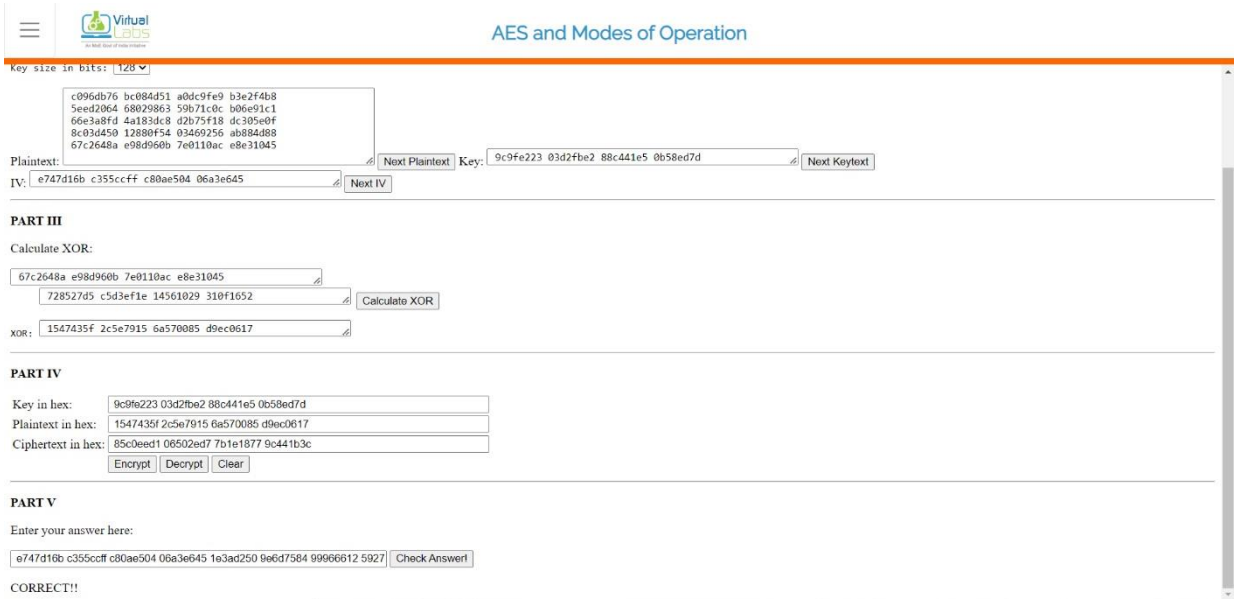


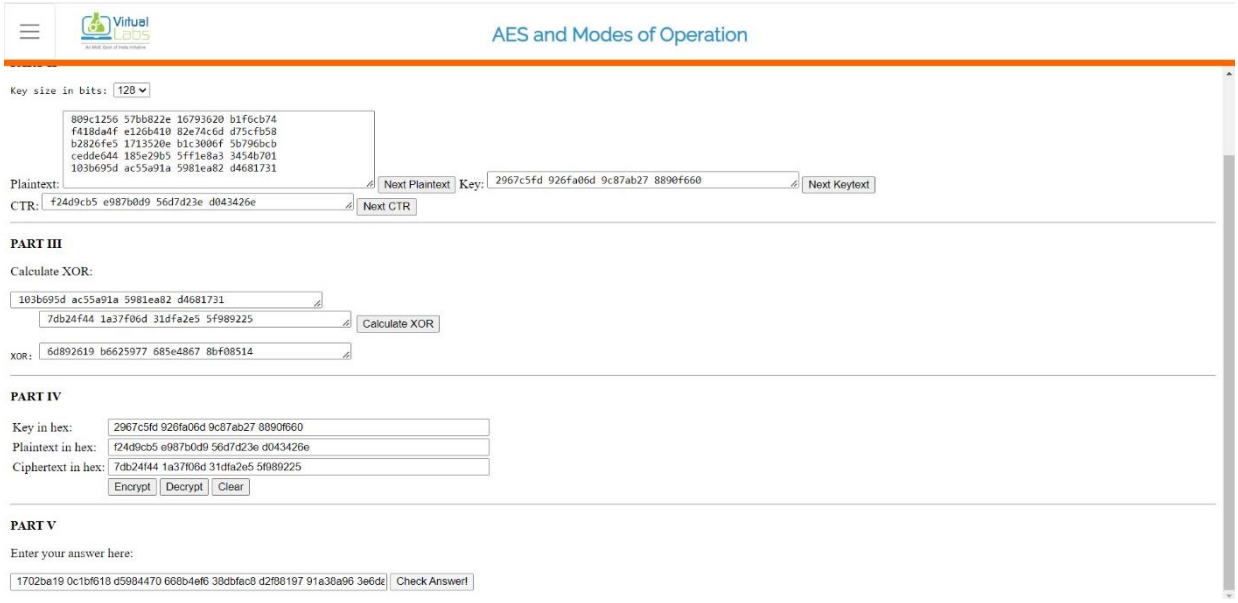

AES and Modes of Operation
Key size in bits: 128
efbfd9b5 16be4bf5 3f4a32ae 18225641
a28e6b05 f9dd6d0e 2ceb4ac6 43e0bcb0
4f4fda79 65b7567c bede510c 3feceea7
5b7befac 25904cc9 e8246988 e1c02e51
4f6a92c1 6607fca4 a1682d56 fbf0b537
Plaintext:
Next Plaintext
Key: 969827e3 18d136da cce9794a 9fe9911c
Next Keytext
IV: d7d68add bc0a6bad 4b16082b 8a62c28a
Next IV
PART III
Calculate XOR:
4f6a92c1 6607fca4 a1682d56 fbf0b537
1f6b8715 33427730 88c30c37 954c1685
Calculate XOR
XOR: 500115d4 55458b94 29ab2161 6ebca3b2
PART IV
Key in hex: 969827e3 18d136da cce9794a 9fe9911c
Plaintext in hex: 0183e3a3 5b614f98 eac112d1 16daea81
Ciphertext in hex: 1f6b8715 33427730 88c30c37 954c1685
Encrypt
Decrypt
Clear
PART V
Enter your answer here:
d7d68add bc0a6bad 4b16082b 8a62c28a 74fb98c8 11c9008d c0dedba0 a29
Check Answer!
CORRECT!!


AES and Modes of Operation
PART I
Choose your mode of operation: Electronic Code Book (ECB)
PART II
Key size in bits: 128
9e02b6c4 6dad8409 a3dc592c 5f49e9c9
5ae4a86a 65c15647 f2b74f22 47dab354
21e25393 4b0a087d 36f79572 f70e32b8
5efe9e6d dd24c2ed 7c941112 9c521b47
b1be277f 63340766 2818260b 135894a9
Plaintext:
Next Plaintext
Key: 9d8c0789 a9a3fede 99b87128 a85c7ee1
Next Keytext
IV:
Next IV
CTR:
Next CTR
PART III
Calculate XOR:
Calculate XOR
XOR:
PART IV
Key in hex: 9d8c0789 a9a3fede 99b87128 a85c7ee1
Plaintext in hex: b1be277f 63340766 2818260b 135894a9
Ciphertext in hex: 44b4ae8b c72b19ac 9f56206a aa0cbe4d


AES and Modes of Operation
9e02b6c4 6dad8409 a3dc592c 5f49e9c9
5ae4a86a 65c15647 f2b74f22 47dab354
21e25393 4b0a087d 36f79572 f70e32b8
5efe9e6d dd24c2ed 7c941112 9c521b47
b1be277f 63340766 2818260b 135894a9
Plaintext:
Next Plaintext
Key: 9d8c0789 a9a3fede 99b87128 a85c7ee1
Next Keytext
IV:
Next IV
CTR:
Next CTR
PART III
Calculate XOR:
Calculate XOR
XOR:
PART IV
Key in hex: 9d8c0789 a9a3fede 99b87128 a85c7ee1
Plaintext in hex: b1be277f 63340766 2818260b 135894a9
Ciphertext in hex: 44b4ae8b c72b19ac 9f56206a aa0cbe4d
Encrypt
Decrypt
Clear
PART V
Enter your answer here:
41b6274c 14cc53f1 6f7af601 c9293182 f742b018 52d5ede3 4397270d 80c21
Check Answer!
CORRECT!!


AES and Modes of Operation
PART I
Choose your mode of operation: Cipher Block Chaining
PART II
Key size in bits: 128
c096db76 bc084d51 a0dc9fe9 b3e2f4b8
5eed2064 68029863 59b71c0c b06e91c1
66e3a8fd 4a183dc8 d2b75f18 dc305e0f
8c03d450 12880f54 03469256 ab884d88
67c2648a e98d960b 7e0110ac e8e31045
Plaintext:
Next Plaintext
Key: 9c9fe223 03d2fbe2 88c441e5 0b58ed7d
Next Keytext
IV: e747d16b c355ccff c80ae504 06a3e645
Next IV
PART III
Calculate XOR:
67c2648a e98d960b 7e0110ac e8e31045
728527d5 c5d3ef1e 14561029 310f1652
Calculate XOR
XOR: 1547435f 2c5e7915 6a570085 d9ec0617
PART IV
Key in hex: 9c9fe223 03d2fbe2 88c441e5 0b58ed7d
Plaintext in hex: 1547435f 2c5e7915 6a570085 d9ec0617
Ciphertext in hex: 85c0eed1 06502ed7 7b1e1877 9c441b3c
Encrypt
Decrypt
Clear





Conclusion:

In conclusion, understanding block cipher modes of operation is essential for secure data encryption. Each mode offers distinct security properties and features. Careful consideration of application requirements is vital to select the most suitable mode, balancing security, performance, and desired functionalities for effective encryption practices.