Roll No 138

Name- Anmol Tripathi

Lab Assignment 3

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

LO2: Demonstrate key management, distribution and user authentication.

THEORY:

Briefly explain AES algorithm (What type of cipher it is? number of rounds, keysize, block size, operations in each round)

The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm that falls under the category of block ciphers. It replaced the older Data Encryption Standard (DES) due to its stronger security features. AES operates on fixed-size blocks of data and is known for its efficiency and resistance against various types of attacks.

<u>Type of Cipher</u>: AES is a symmetric key block cipher, which means the same secret key is used for both encryption and decryption. It transforms plaintext blocks into ciphertext blocks using a series of complex operations.

<u>Number of Rounds</u>: AES operates with different numbers of rounds depending on the key size:

AES-128: 10 rounds

AES-192: 12 rounds

AES-256: 14 rounds

<u>Key Size</u>: AES supports key sizes of 128, 192, or 256 bits. The security and strength of the encryption increase with larger key sizes.

<u>Block Size</u>: AES operates on fixed-size blocks of 128 bits.

<u>Operations in Each Round:</u>

SubBytes: Non-linear substitution of each byte in the block using a predefined substitution table (S-box).

ShiftRows: Byte shifting within each row to provide diffusion in the data.

MixColumns: Mixing operation that transforms columns of data to provide diffusion across columns.

AddRoundKey: Each byte of the block is combined with the corresponding round key derived from the original encryption key.

These operations are applied repeatedly for the specified number of rounds, with each round using a different round key. The complex interaction of these operations ensures that even a small change in the plaintext results in a significantly different ciphertext, a property known as the avalanche effect. This contributes to the security and robustness of AES against various cryptographic attacks.

With diagram explain in brief block cipher modes of operation

ECB mode

CBC mode

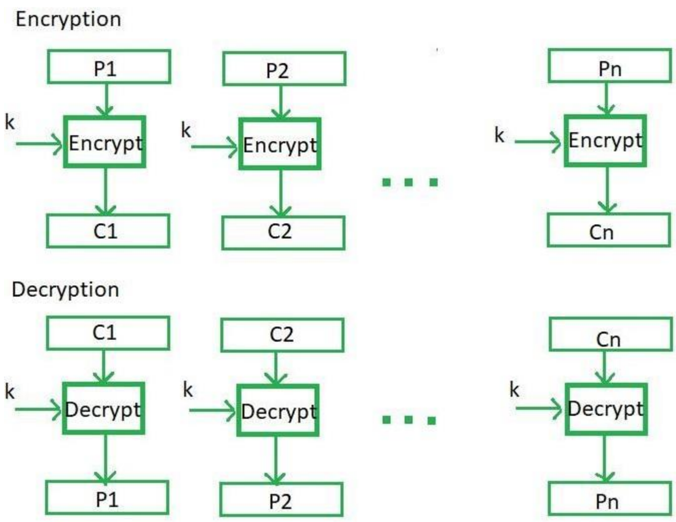
OFB mode

Counter mode

Block cipher modes of operation are techniques used to apply a block cipher, like AES, to encrypt or decrypt data that is larger than the block size of the cipher. These modes define how blocks of plaintext are transformed into ciphertext and vice versa. Here's a brief explanation of some common block cipher modes of operation:

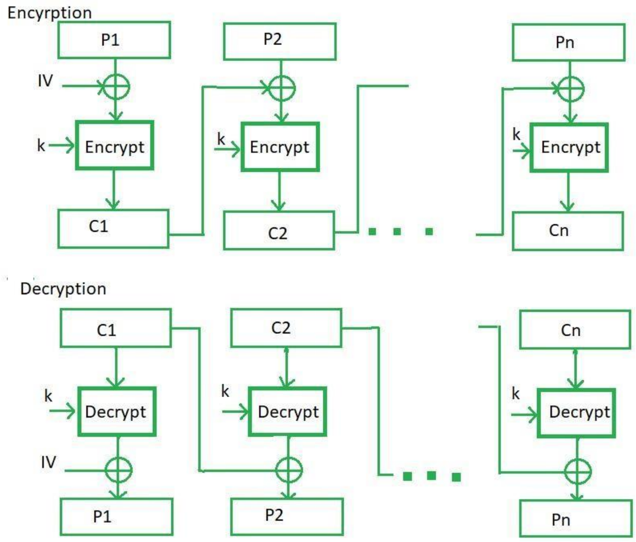
Electronic Codebook (ECB) Mode:

ECB mode is the simplest mode, where each block of plaintext is independently encrypted using the same encryption key. However, this mode has a significant limitation: identical plaintext blocks result in identical ciphertext blocks, making it vulnerable to certain attacks. ECB mode is not suitable for encrypting large amounts of data or data with patterns.



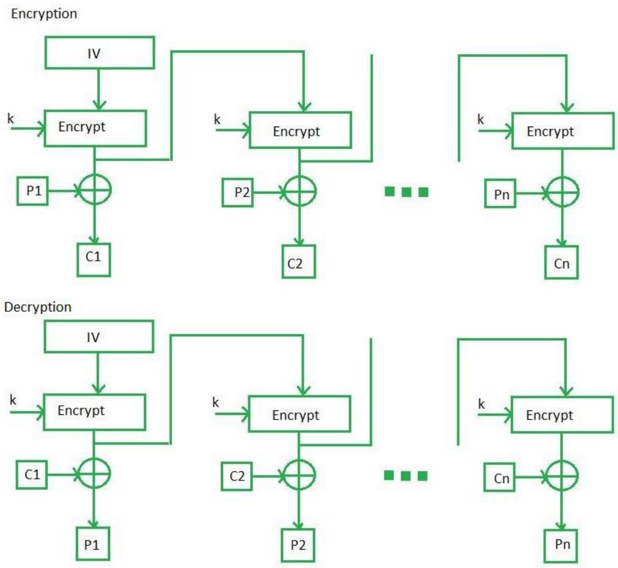
Cipher Block Chaining (CBC) Mode:

In CBC mode, each plaintext block is XORed with the previous ciphertext block before encryption. This introduces a form of feedback, where the ciphertext from the previous block affects the encryption of the current block. Initialization Vector (IV) is used to start the process. CBC mode prevents identical plaintext blocks from producing identical ciphertext blocks and provides a basic level of security. Decryption requires the previous ciphertext block to be available.



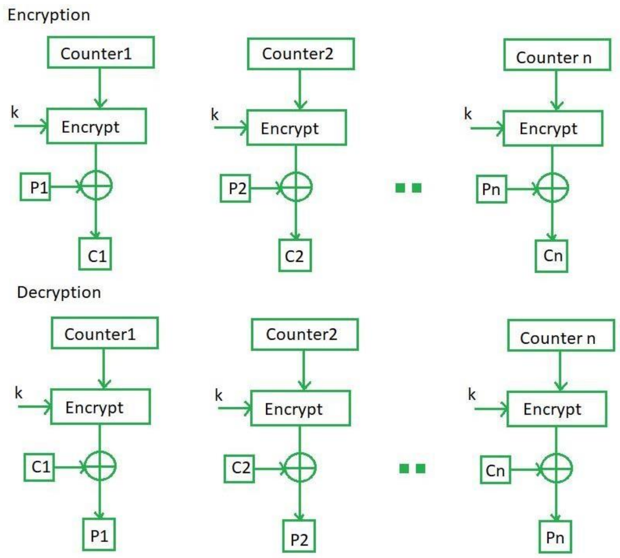
Output Feedback (OFB) Mode:

OFB mode converts a block cipher into a stream cipher. It generates a keystream using the encryption of an IV and successive values (feedback) derived from the encryption of the previous block's ciphertext. The keystream is XORed with the plaintext to produce the ciphertext and vice versa. OFB mode does not require decryption in the encryption process and is suitable for applications where error propagation is a concern.



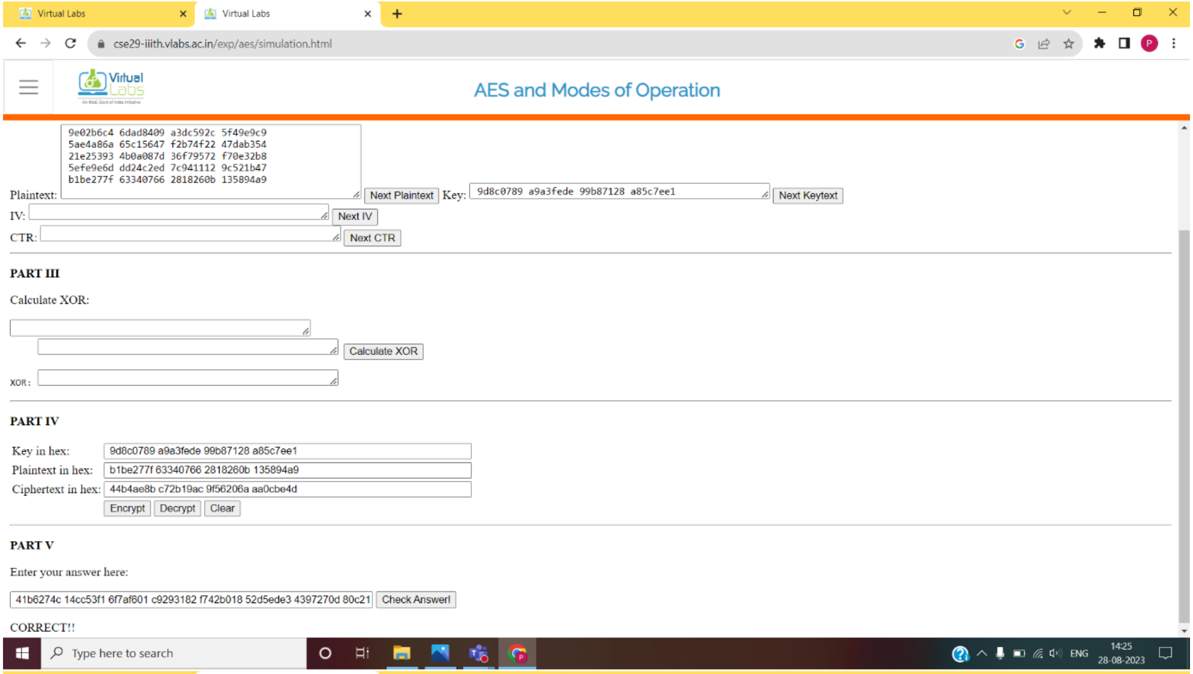
Counter (CTR) Mode:

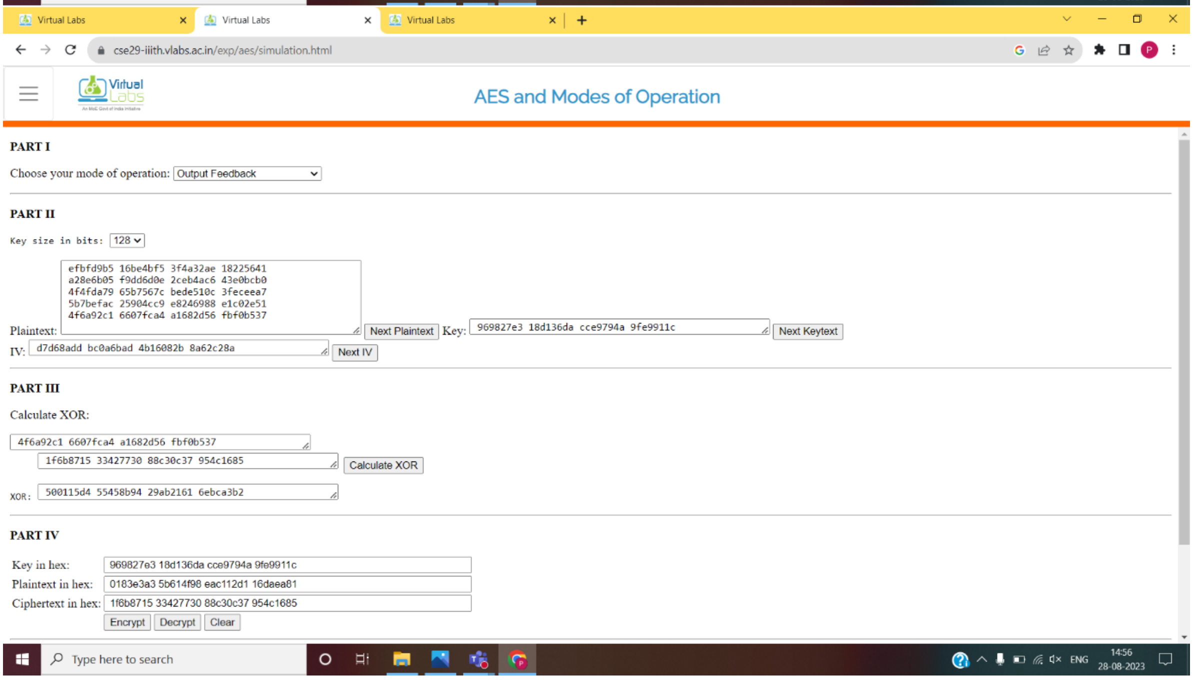
CTR mode also turns a block cipher into a stream cipher. It involves encrypting a counter value using the encryption key, and the resulting output is XORed with the plaintext to produce the ciphertext. The counter value is incremented for each block. CTR mode allows for parallel encryption and decryption, making it efficient for multi-core processors. It also offers excellent error propagation.

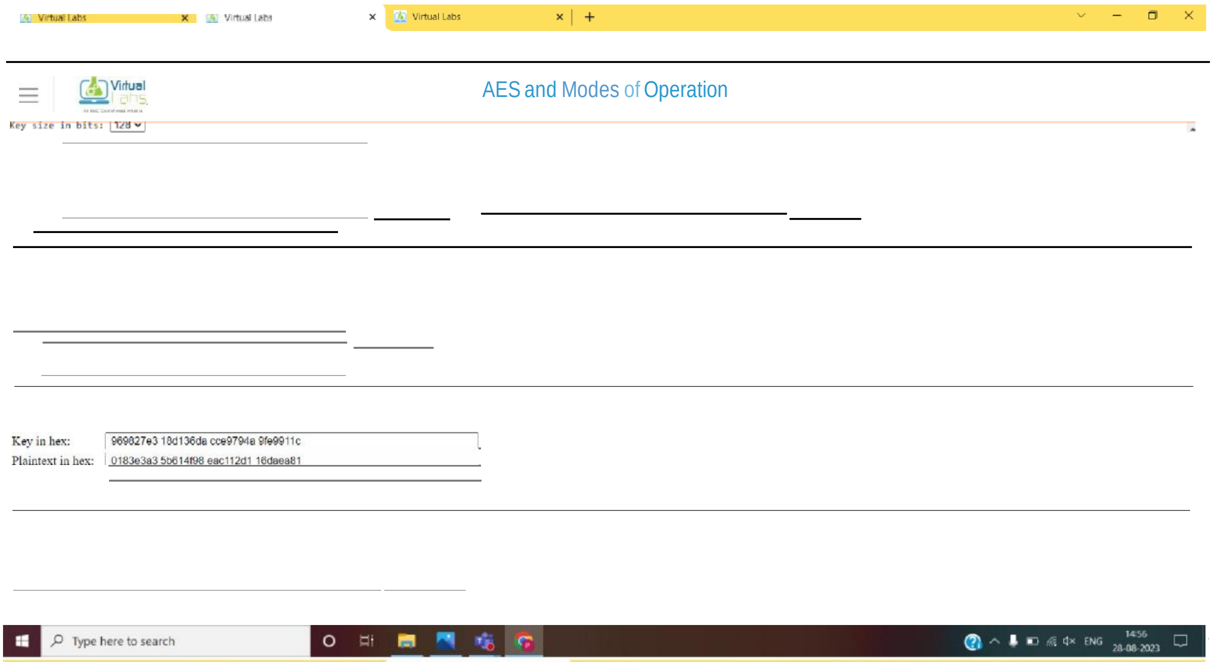


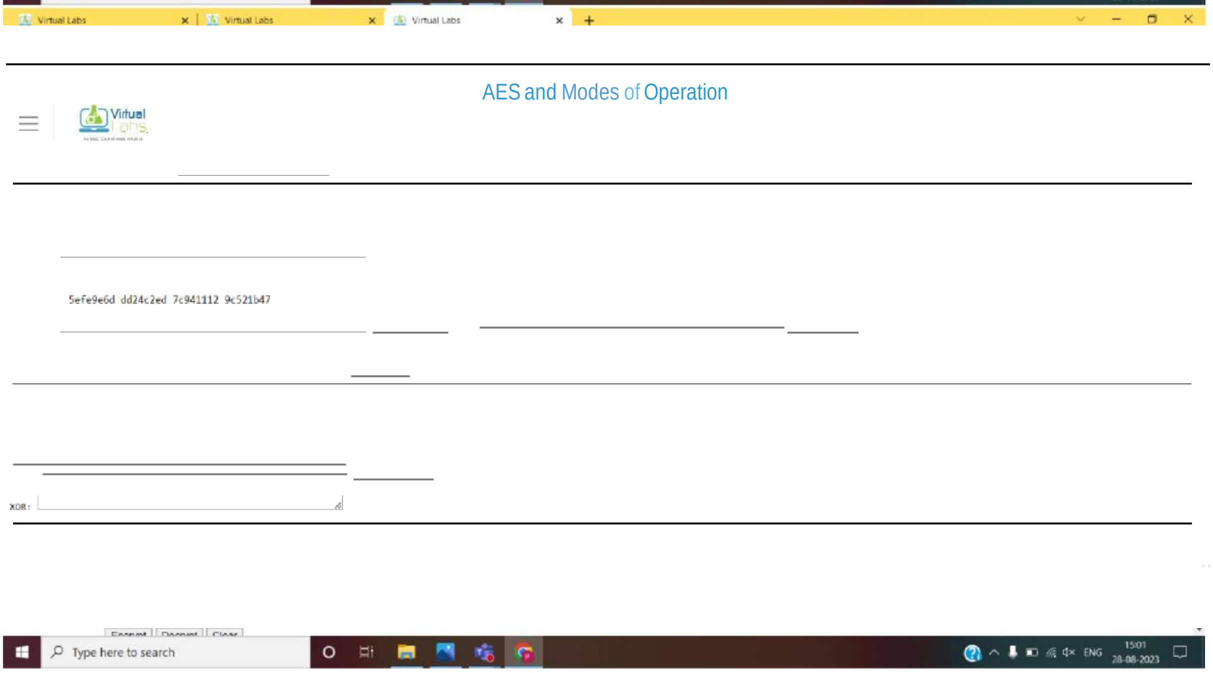
These modes provide different trade-offs between security, performance, and error propagation. It's important to choose the appropriate mode based on the specific requirements of your application. Additionally, some modes, like CBC and CTR, require the use of Initialization Vectors (IVs) to ensure uniqueness and security of the encryption process.

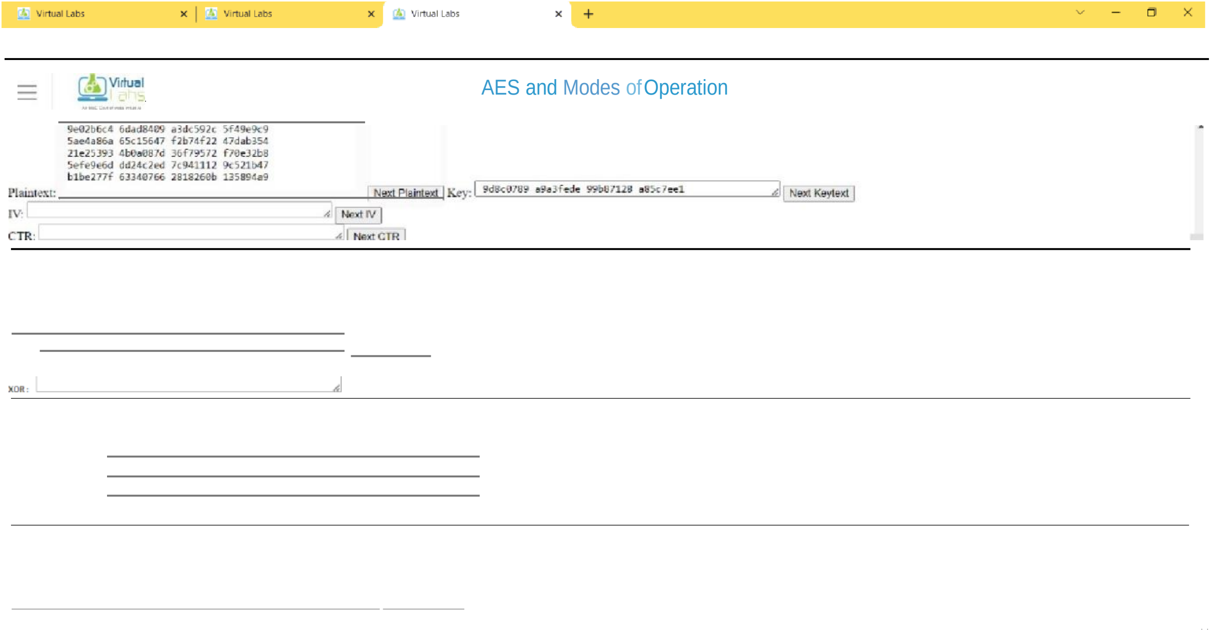
OUTPUT


Virtual Labs
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
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!!
Type here to search
ENG
14:25
28-08-2023

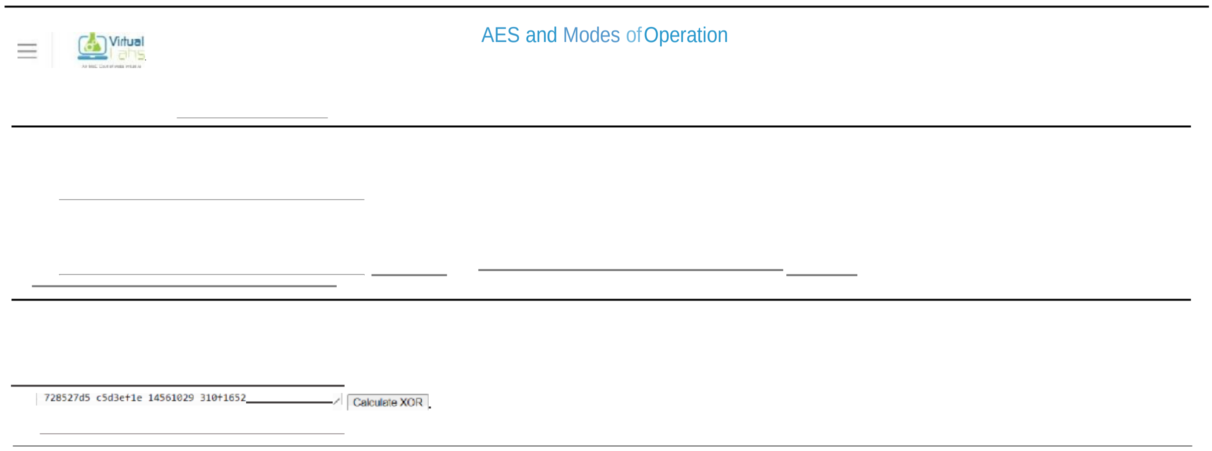

Virtual Labs
Virtual Labs
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
AES and Modes of Operation
PART I
Choose your mode of operation: Output Feedback
PART II
Key size in bits: 128
efbfd9b5 16be4bf5 3f4a32ae 18225641
a28e6b05 f9dd6d0e 2ceb4ac6 43e0bcb0
4f4fda79 65b7567c bede510c 3feceea7
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
Type here to search
ENG
14:56
28-08-2023

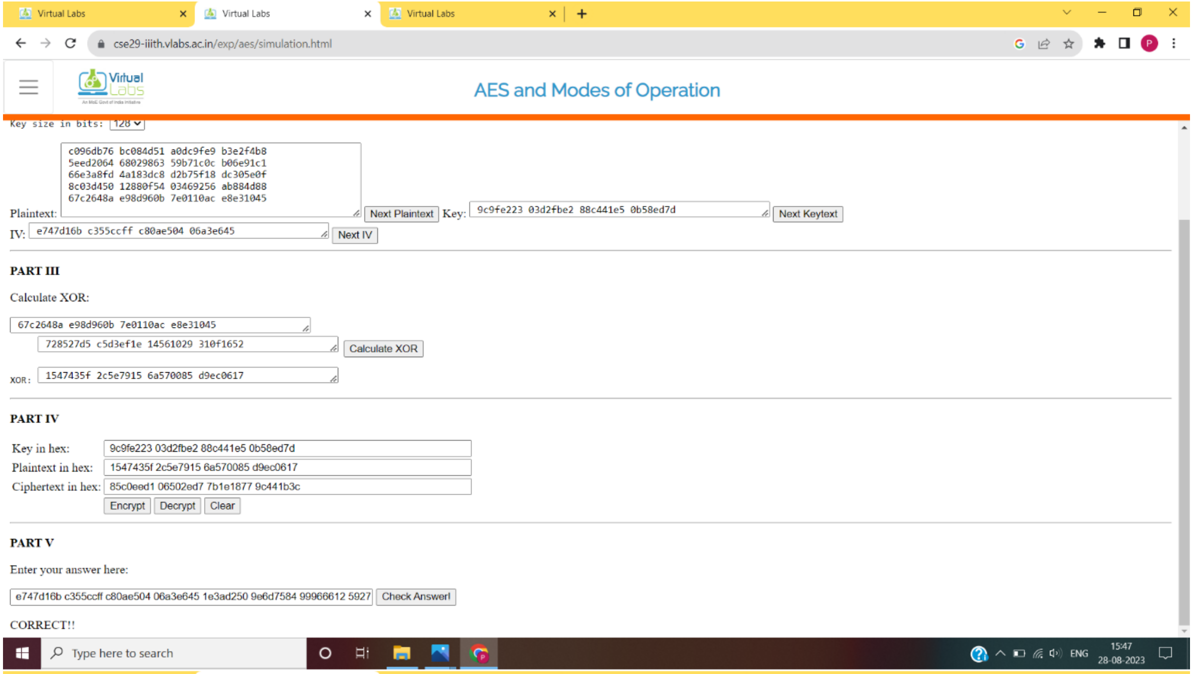

Virtual Labs
AES and Modes of Operation
Key size in bits: 128
Key in hex: 969827e3 18d136da cce9794a 9fe9911c
Plaintext in hex: 0183e3a3 5b614f98 eac112d1 16daea81
Type here to search
ENG
14:56
28-08-2023


Virtual Labs
AES and Modes of Operation
5efe9e6d dd24c2ed 7c941112 9c521b47
XOR:
Type here to search
ENG
15:01
28-08-2023

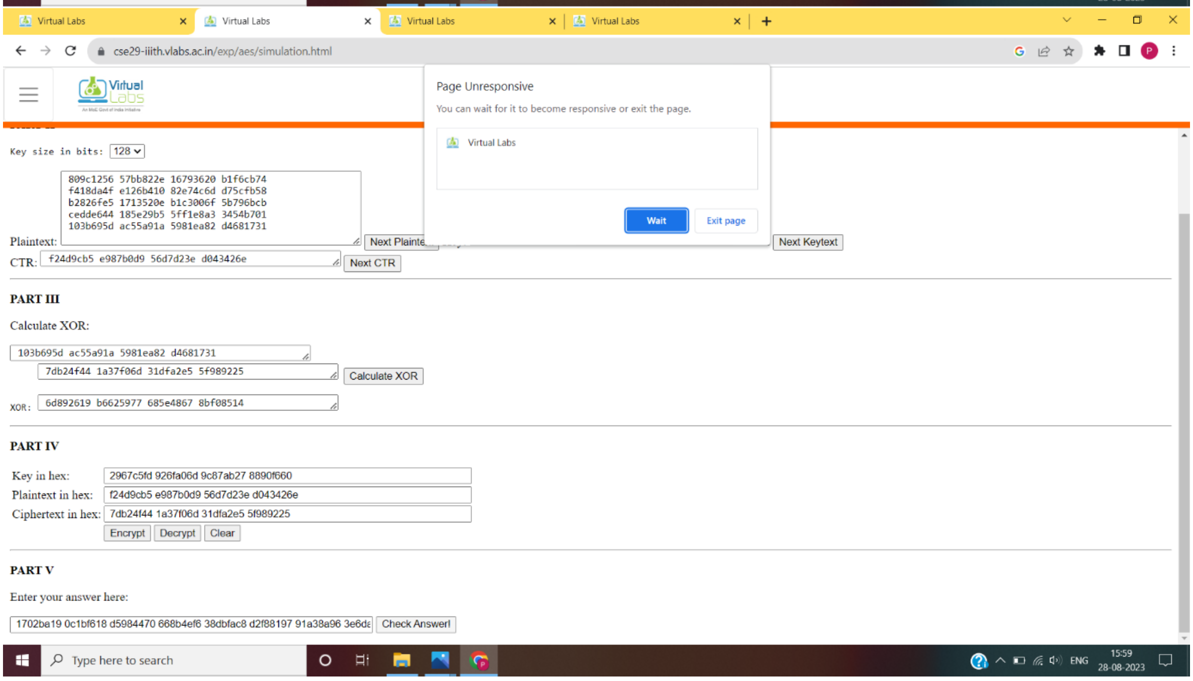

Virtual Labs
Virtual Labs
Virtual Labs
Virtual Labs
AES and Modes of Operation
9e02b6c4 6dad8409 a3dc592c 5f49e9c9
5ae4a86a 65c15647 f2b74f22 47dab354
21e25393 4b0a087d 36f79572 f70e32b8
5efe9e6d dd24c2ed 7c941112 9c521b47
b1be277f 63340766 2818260b 135894a9
Plaintext:
Next Plaintext
Key:
9d8c0789 a9a3fede 99b87128 a85c7ee1
Next Keytext
IV:
Next IV
CTR:
Next CTR
XOR :

[redacted]

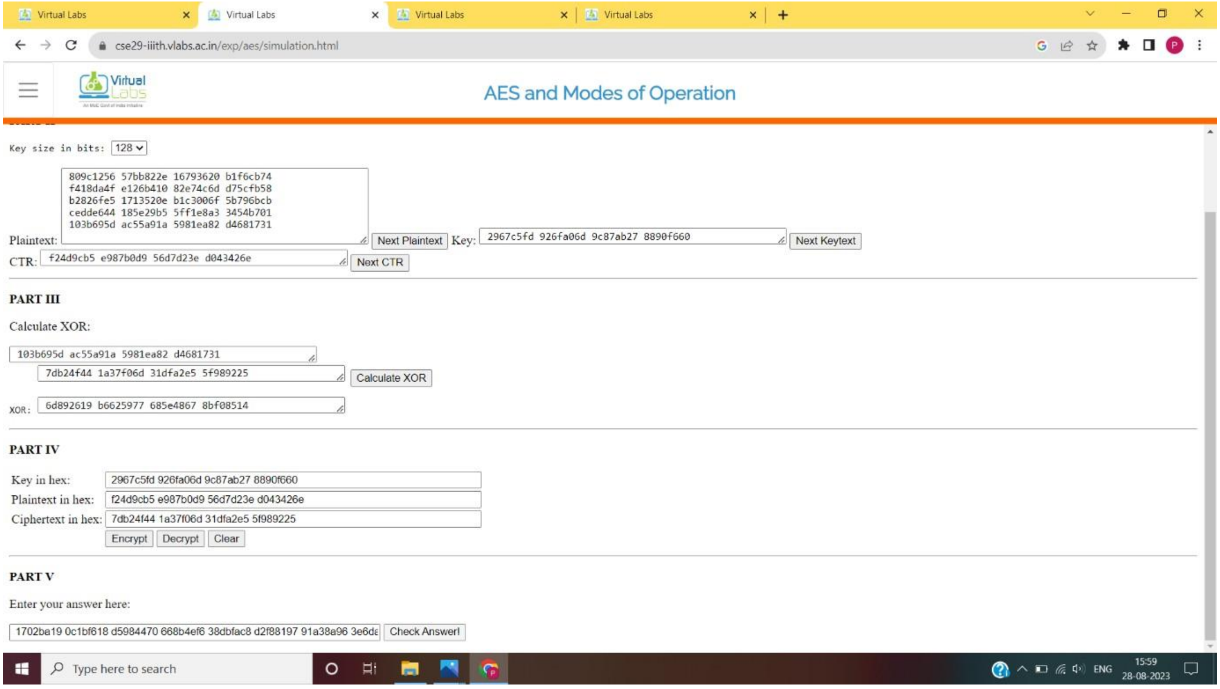

Virtual Labs
AES and Modes of Operation
728527d5 c5d3e+1e 14561029 310+1652
Calculate XOR



Virtual Labs
Virtual Labs
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
Virtual Labs
AES and Modes of Operation
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
PART V
Enter your answer here:
e747d16b c355ccff c80ae504 06a3e645 1e3ad250 9e6d7584 99966612 5927
Check Answer!
CORRECT!!
Type here to search
ENG
15:47
28-08-2023



Virtual Labs
Virtual Labs
Virtual Labs
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
Virtual Labs
Page Unresponsive
You can wait for it to become responsive or exit the page.
Virtual Labs
Wait
Exit page
Key size in bits: 128
809c1256 57bb822e 16793620 b1f6cb74
f418da4f e126b410 82e74c6d d75cfb58
b2826fe5 1713520e b1c3006f 5b796bcb
cedde644 185e29b5 5ff1e8a3 3454b701
103b695d ac55a91a 5981ea82 d4681731
Plaintext:
Next Keytext
CTR: f24d9cb5 e987b0d9 56d7d23e d043426e
Next CTR
PART III
Calculate XOR:
103b695d ac55a91a 5981ea82 d4681731
7db24f44 1a37f06d 31dfa2e5 5f989225
Calculate XOR
XOR: 6d892619 b6625977 685e4867 8bf08514
PART IV
Key in hex: 2967c5fd 926fa06d 9c87ab27 8890f660
Plaintext in hex: f24d9cb5 e987b0d9 56d7d23e d043426e
Ciphertext in hex: 7db24f44 1a37f06d 31dfa2e5 5f989225
Encrypt
Decrypt
Clear
PART V
Enter your answer here:
1702ba19 0c1bf618 d5984470 668b4ef6 38dbfac8 d2f88197 91a38a96 3e6d
Check Answer!
Type here to search
ENG
15:59
28-08-2023



CONCLUSION:

The AES experiment offered a practical glimpse into the world of symmetric key cryptography. We explored AES's encryption processes, recognizing its efficiency and adaptability for secure data handling. By employing different modes of operation, such as ECB, CBC, OFB, and Counter, we comprehended the distinct trade-offs between security, performance, and error propagation.