Roll Number:- 2105048
Name:-Manav Jain
Date:- 09/08/2023

Lab Assignment No:-3

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

Lab Outcome Attained :- LO2

Theory:-

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

Advanced Encryption Standard (AES) is a symmetric-key block cipher that is used to encrypt and decrypt data. It is a substitution-permutation network (SPN) cipher, which means that it works by repeatedly substituting and permuting the input data.

Key features of AES:

1)Type of cipher: Symmetric-key block cipher
2)Number of rounds: 10, 12, or 14 rounds, depending on the key size
3)Keysize: 128, 192, or 256 bits
4)Block size: 128 bits
5)Operations in each round:
  Byte substitution (SubBytes)
  Shift rows (ShiftRows)
  Mix columns (MixColumns)

Add round key (AddRoundKey)

The AES algorithm is considered to be very secure and has been adopted by many organizations and governments around the world. It is used to protect sensitive data in a variety of applications, including:

Email

File encryption

Disk encryption

Wireless networking

Cloud computing

Operations performed in each round of AES:

Byte substitution (SubBytes): This operation replaces each byte in the input block with a new byte that is selected from a lookup table. This table is designed to make the cipher resistant to attacks based on frequency analysis.

Shift rows (ShiftRows): This operation cyclically shifts the rows of the input block by different amounts. This operation makes the cipher resistant to attacks based on differential cryptanalysis.

Mix columns (MixColumns): This operation mixes the columns of the input block using a linear transformation. This operation makes the cipher resistant to attacks based on linear cryptanalysis.

Add round key (AddRoundKey): This operation XORs the input block with the round key. This operation ensures that each round of the cipher depends on the previous rounds, which makes it more difficult to break.

The number of rounds in AES depends on the key size. For a 128-bit key, there are 10 rounds. For a 192-bit key, there are 12 rounds. And for a 256-bit key, there are 14 rounds.

The AES algorithm is a very secure and efficient cipher that is widely used around the world

With diagram explain in brief block cipher modes of operation

1) ECB mode

2) CBC mode

3) OFB mode

4) Counter mode

1)ECB (Electronic Code Book)

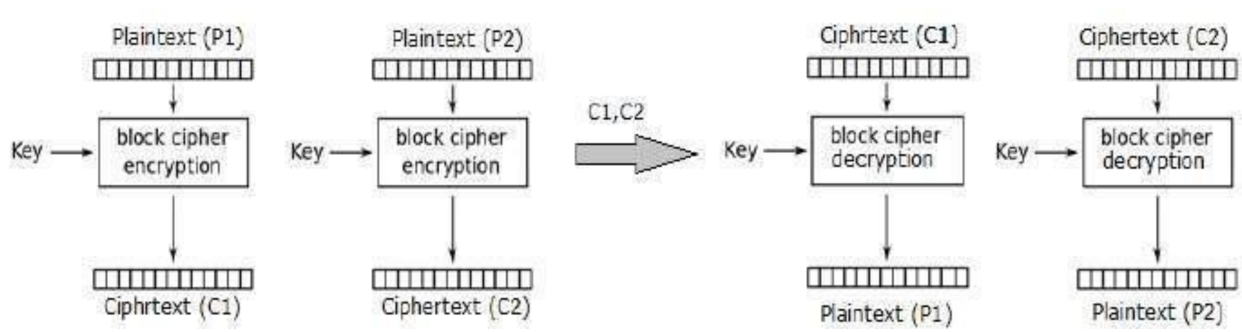
This mode is a most straightforward way of processing a series of sequentially listed message blocks.

Operation

The user takes the first block of plaintext and encrypts it with the key to produce the first block of ciphertext.He then takes the second block of plaintext and follows the same process with same key and so on so forth.

The ECB mode is deterministic, that is, if plaintext block P1, P2,…, Pm are encrypted twice under the same key, the output ciphertext blocks will be the same.

In fact, for a given key technically we can create a codebook of ciphertexts for all possible plaintext blocks. Encryption would then entail only looking up for required plaintext and select the corresponding ciphertext. Thus, the operation is analogous to the assignment of code words in a codebook, and hence gets an official name − Electronic Codebook mode of operation (ECB). It is illustrated as follows −



2)CBC mode(cipher block chaining)

CBC mode of operation provides message dependence for generating ciphertext and makes the system non-deterministic.

Operation

The operation of CBC mode is depicted in the following illustration. The steps are as follows −

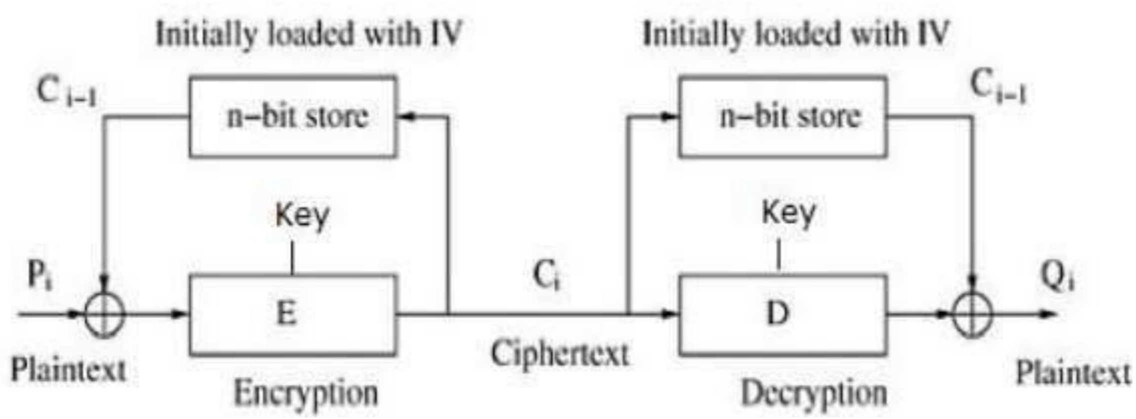
Load the n-bit Initialization Vector (IV) in the top register.

XOR the n-bit plaintext block with data value in top register.

Encrypt the result of XOR operation with underlying block cipher with key K.

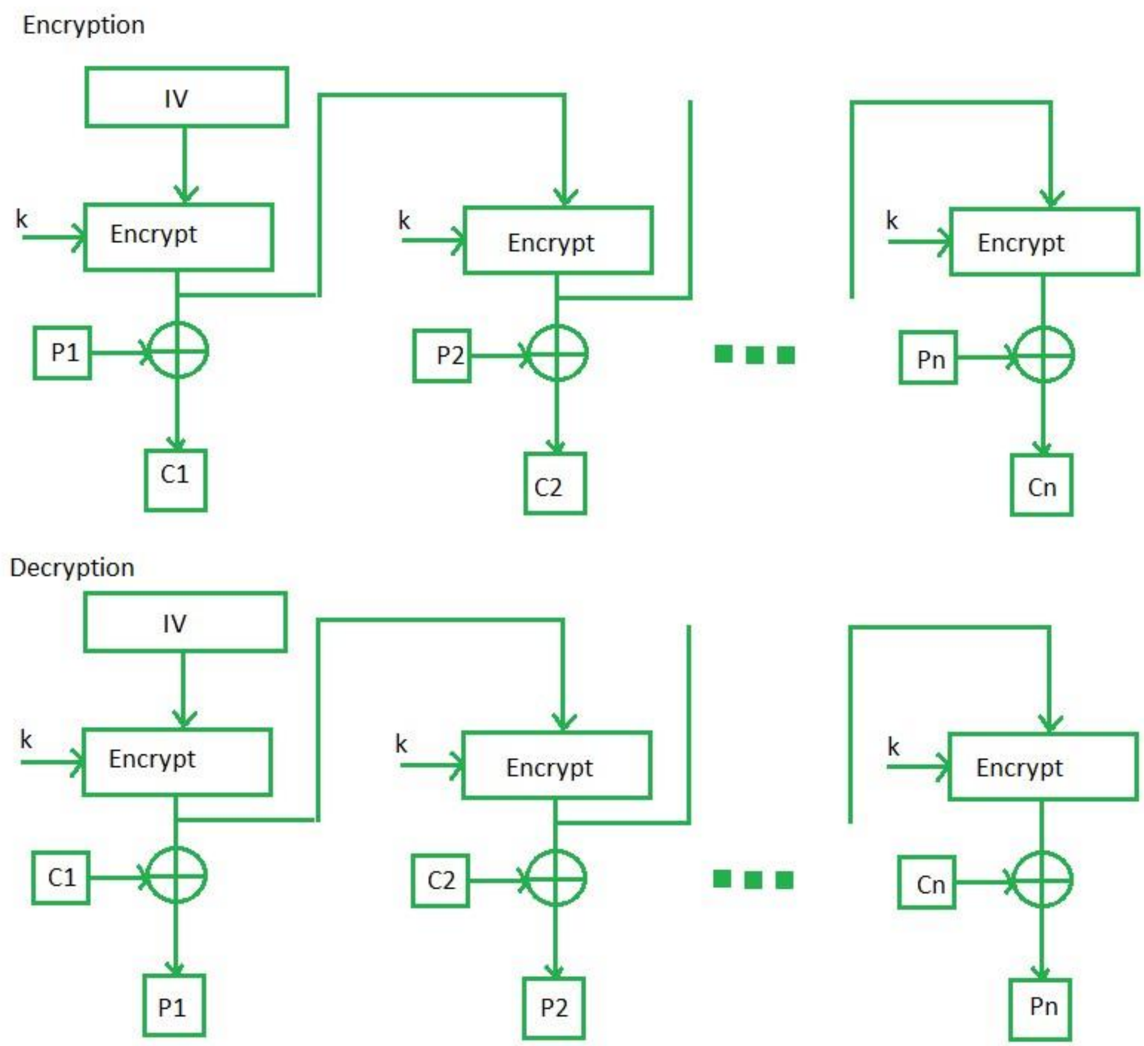
Feed ciphertext block into top register and continue the operation till all plaintext blocks are processed.

For decryption, IV data is XORed with first ciphertext block decrypted. The first ciphertext block is also fed into to register replacing IV for decrypting next ciphertext block.



3)OFB mode(output feedback mode)

OFB Mode stands for output feedback Mode. OFB mode is similar to CFB mode; the only difference is in CFB, the ciphertext is used for the next stage of the encryption process, whereas in OFB, the output of the IV encryption is used for the next stage of the encryption process.The IV is encrypted using the key and form encrypted IV. Plain text and leftmost 8 bits of encrypted IV are combined using XOR and produce the ciphertext.For the next stage, the ciphertext, which is the form in the previous stage, is used as an IV for the next iteration. The same procedure is followed for all blocks.



4)Counter(CTR) mode

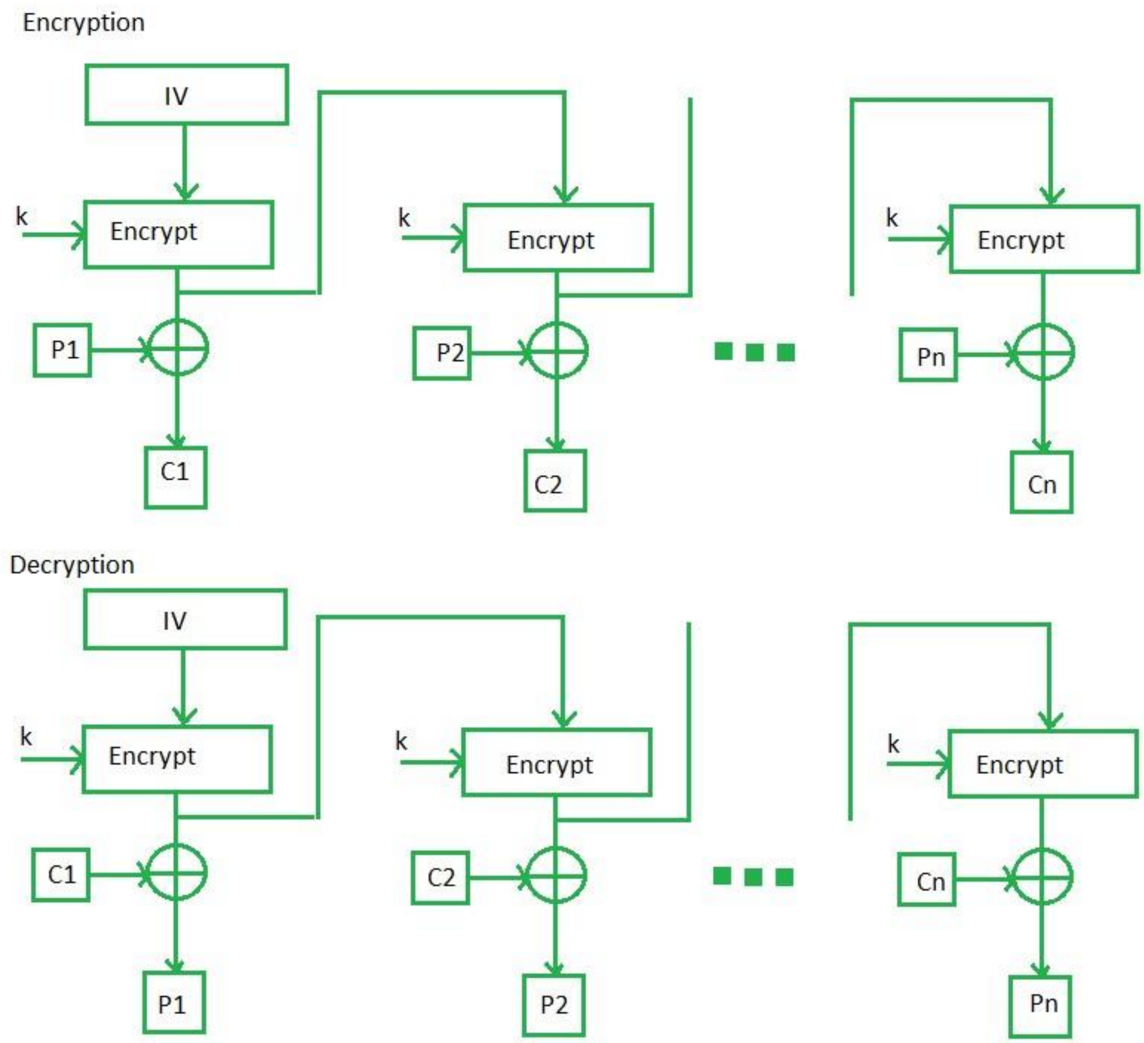
It can be considered as a counter-based version of CFB mode without the feedback. In this mode, both the sender and receiver need to access to a reliable counter, which computes a new shared value each time a ciphertext block is exchanged. This shared counter is not necessarily a secret value, but challenge is that both sides must keep the counter synchronized.

Operation

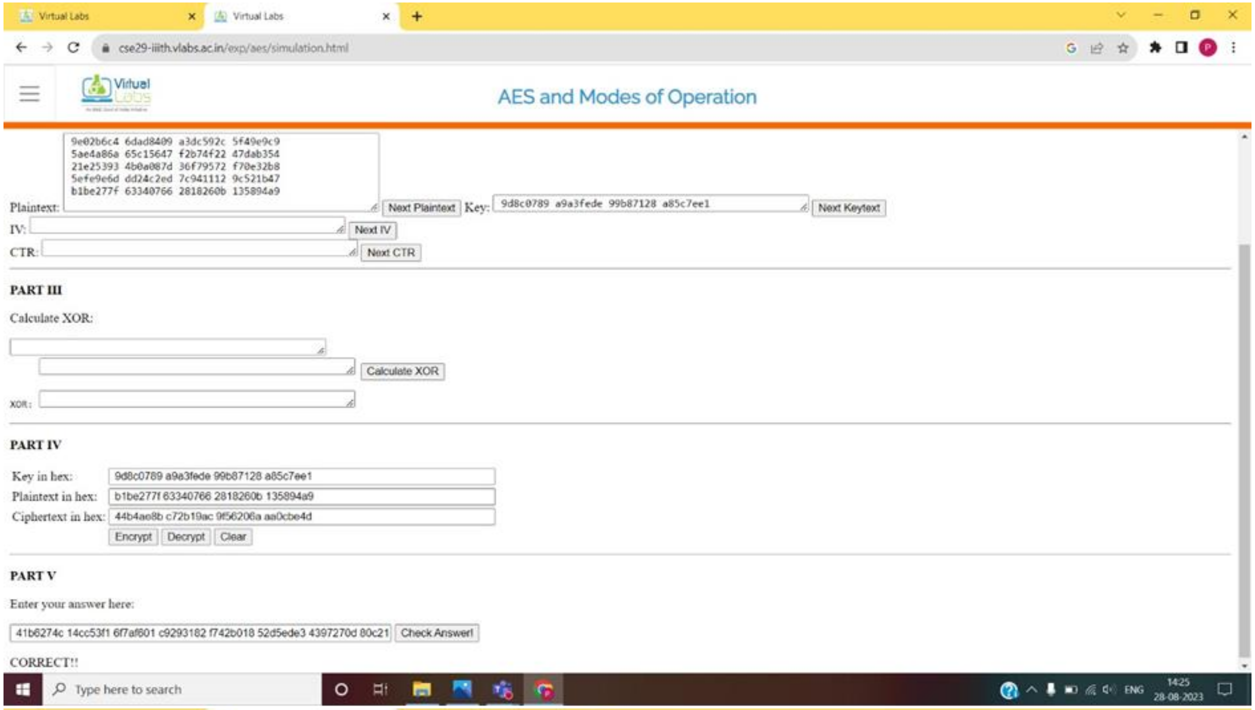
Both encryption and decryption in CTR mode are depicted in the following illustration. Steps in operation are −

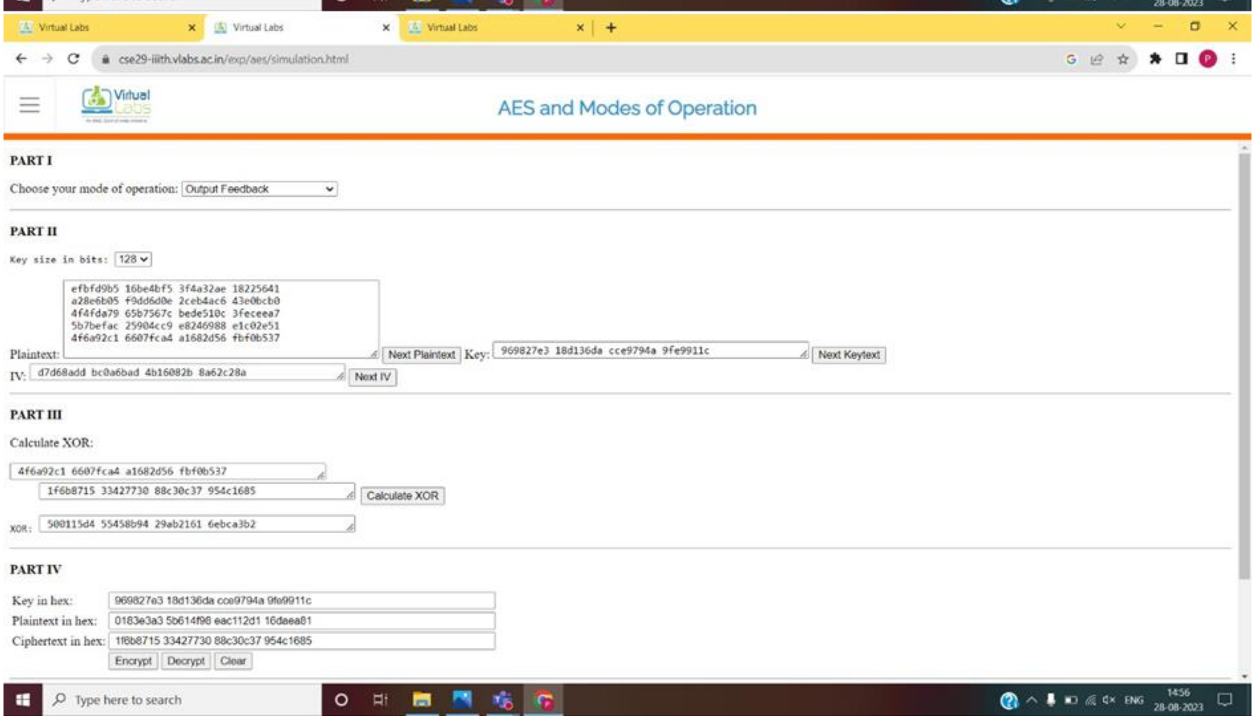
Load the initial counter value in the top register is the same for both the sender and the receiver. It plays the same role as the IV in CFB (and CBC) mode.Encrypt the contents of the counter with the key and place the result in the bottom register.

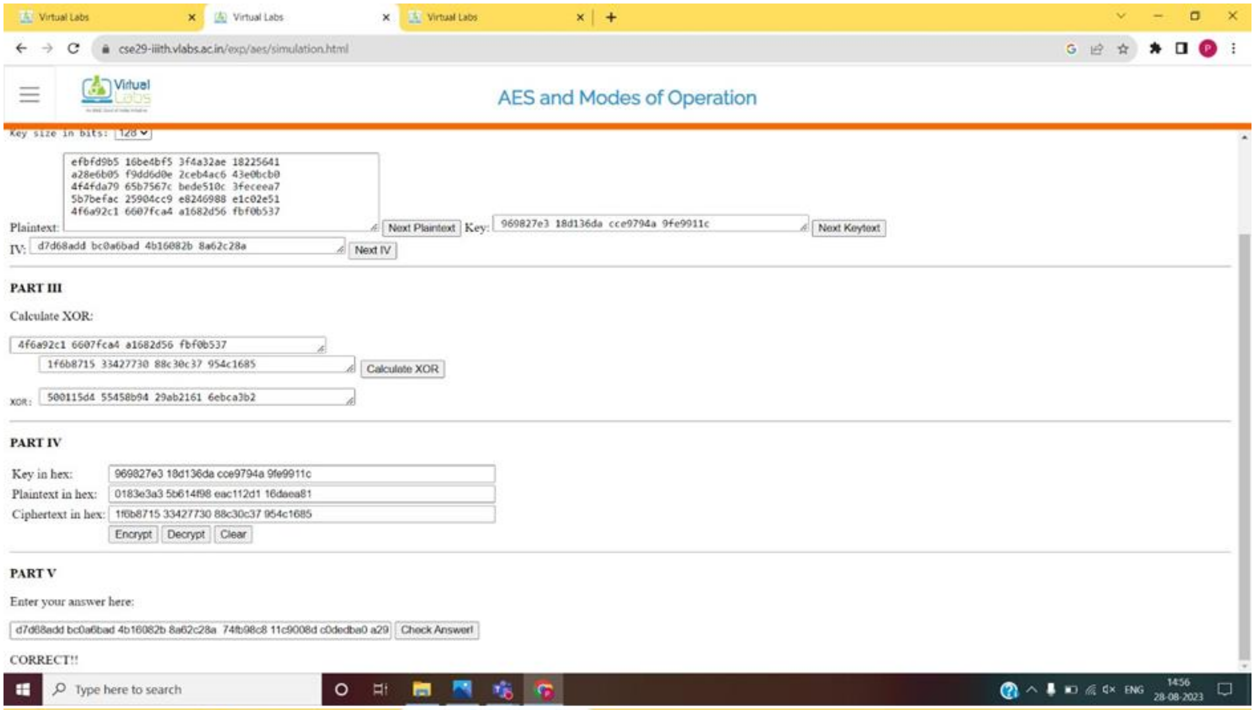
Take the first plaintext block P1 and XOR this to the contents of the bottom register. The result of this is C1. Send C1 to the receiver and update the counter. The counter update replaces the ciphertext feedback in CFB mode.Continue in this manner until the last plaintext block has been encrypted.The decryption is the reverse process. The ciphertext block is XORed with the output of encrypted contents of counter value. After decryption of each ciphertext block counter is updated as in case of encryption.

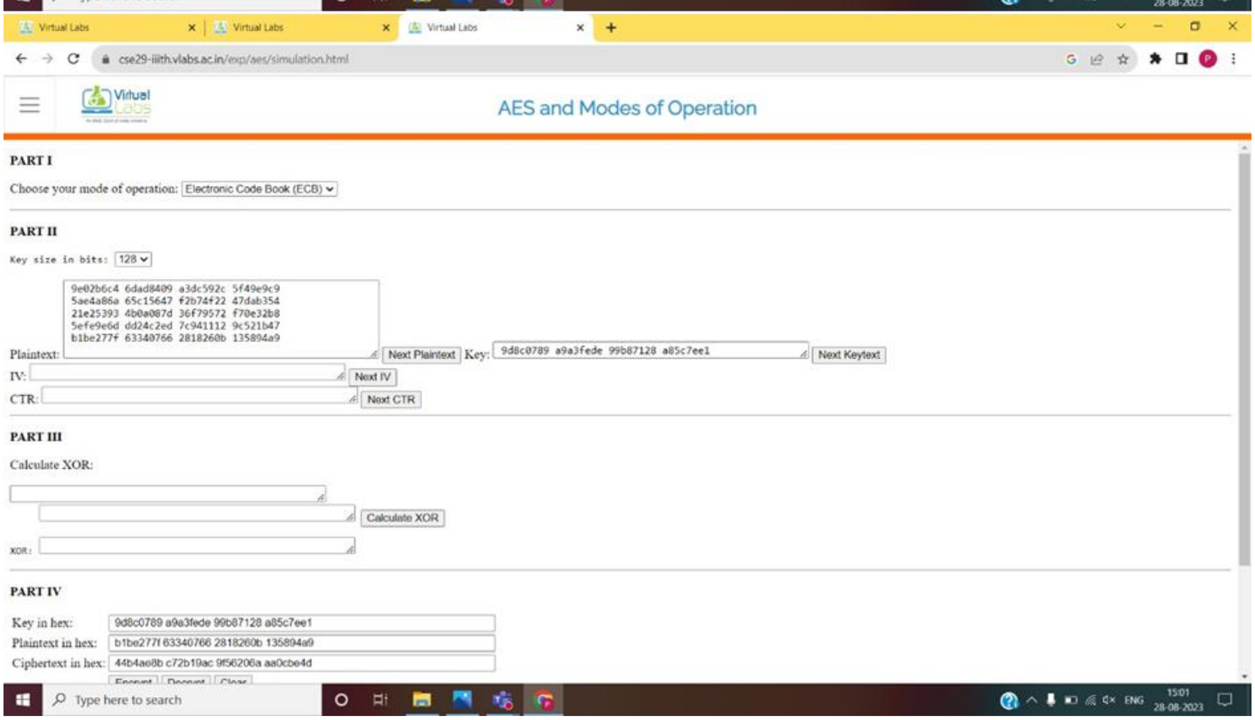


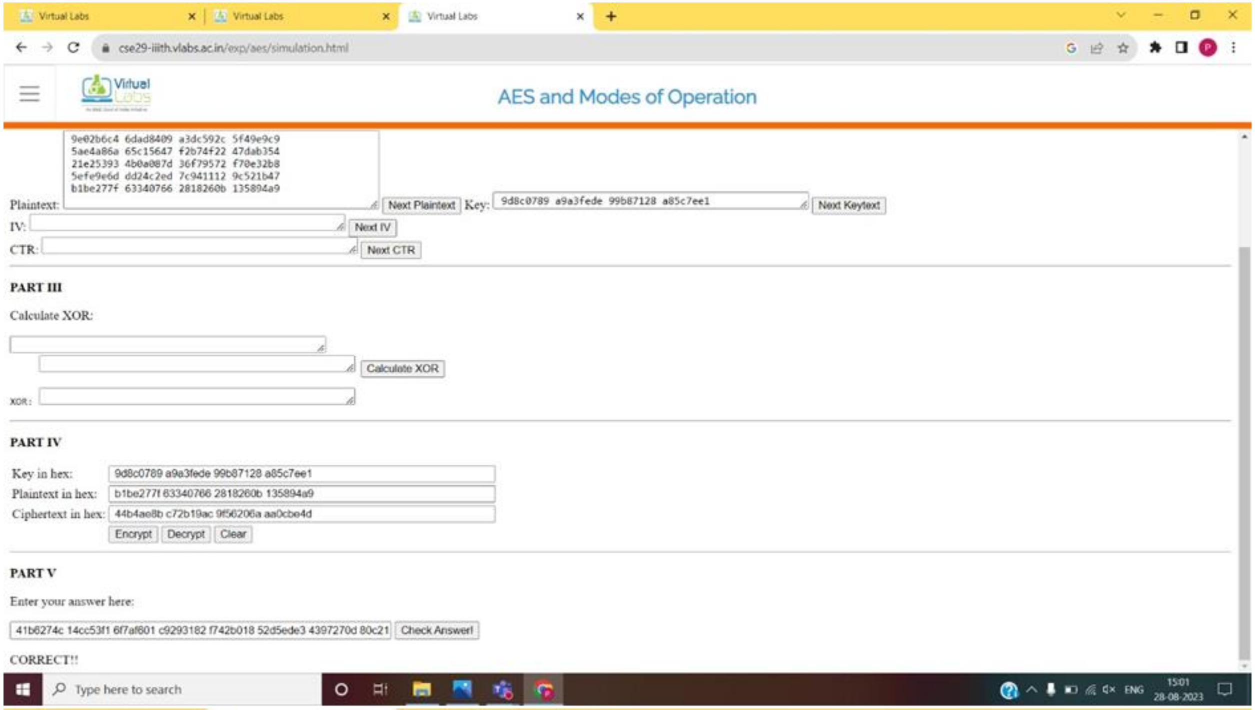
Output Screenshot:-

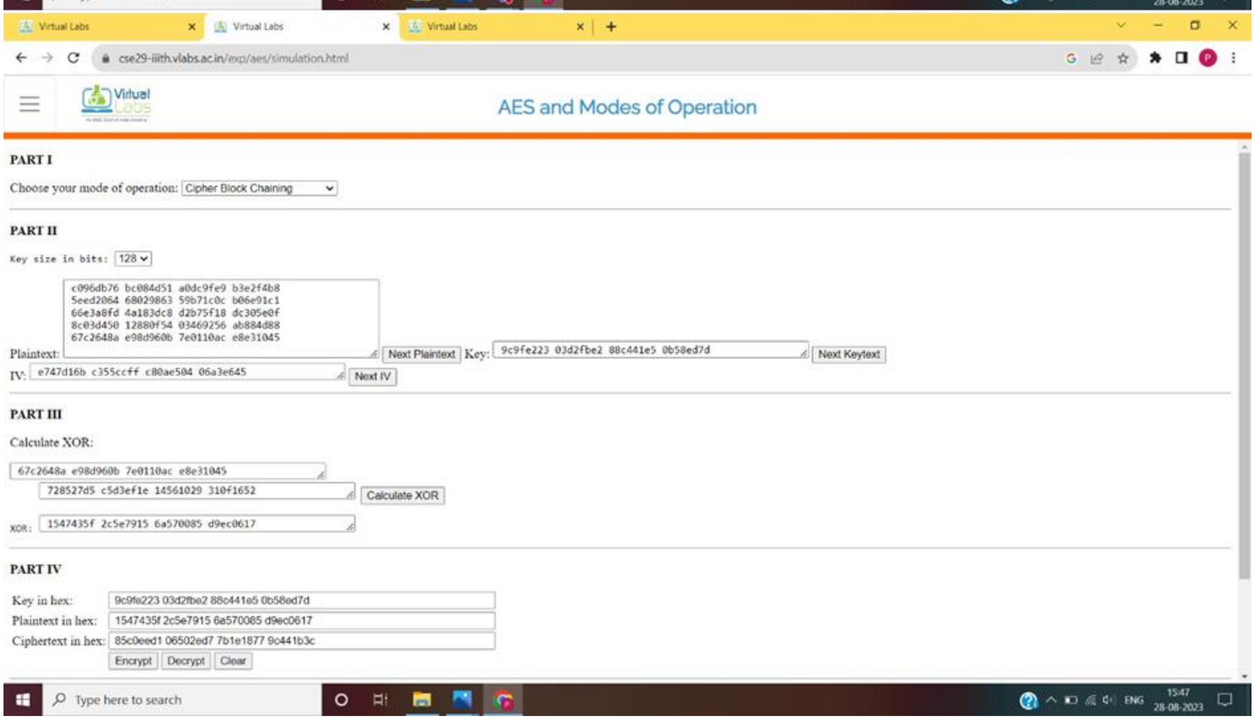

Virtual Labs
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
AES and Modes of Operation
9e02b6c4 6dad8409 a3dc592c 5f49e9c9
5ae4a86a 65c15647 f2b74f22 47dab354
21e25393 4b0a087d 36f79572 f70e32b8
5efe9e6d dd24c2ed 7c941112 9c521b47
b1be277f 63340766 2818260b 135894a9
Plaintext:
Next Plaintext
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

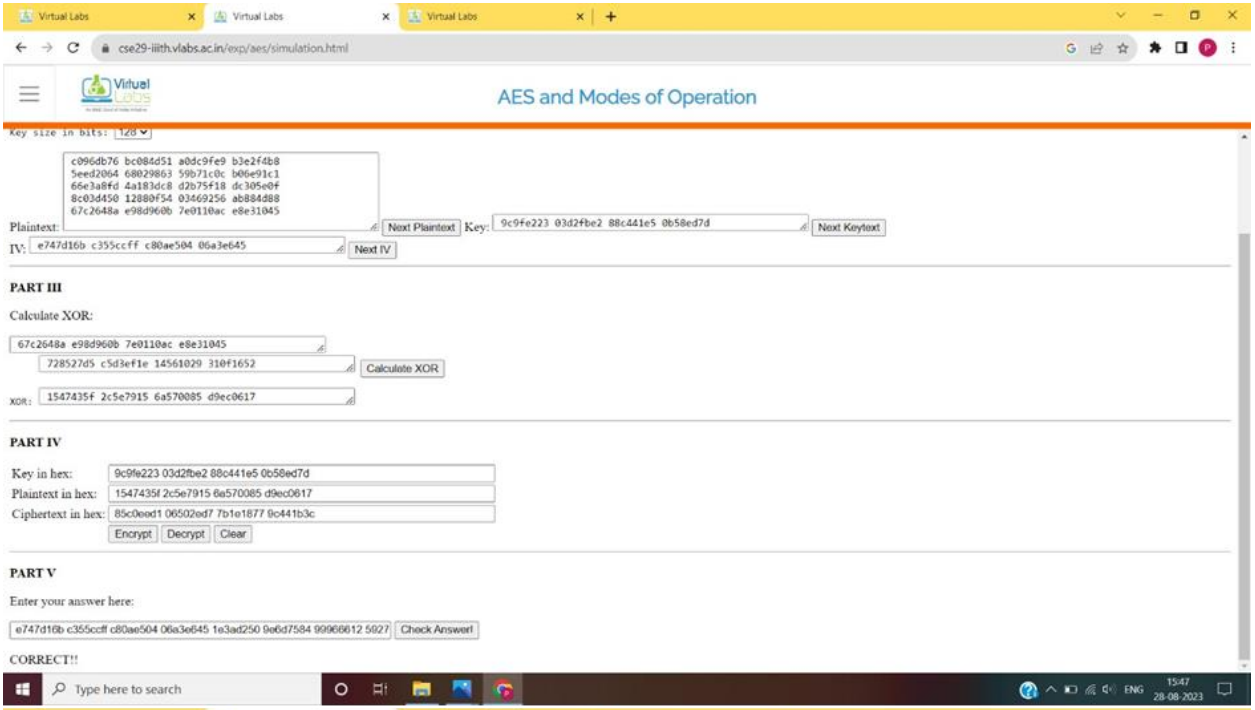

Virtual Labs
Virtual Labs
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
AES and Modes of Operation
PART I
Choose your mode of operation: Output Feedback
PART II
Key size in bits: 128
efbfd9b5 16be4bf5 3f4a32ae 18225641
a28e6b05 f9dd6d0e 2ceb4ac6 43e0bcb0
4f4fda79 65b7567c bede510c 3feceea7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

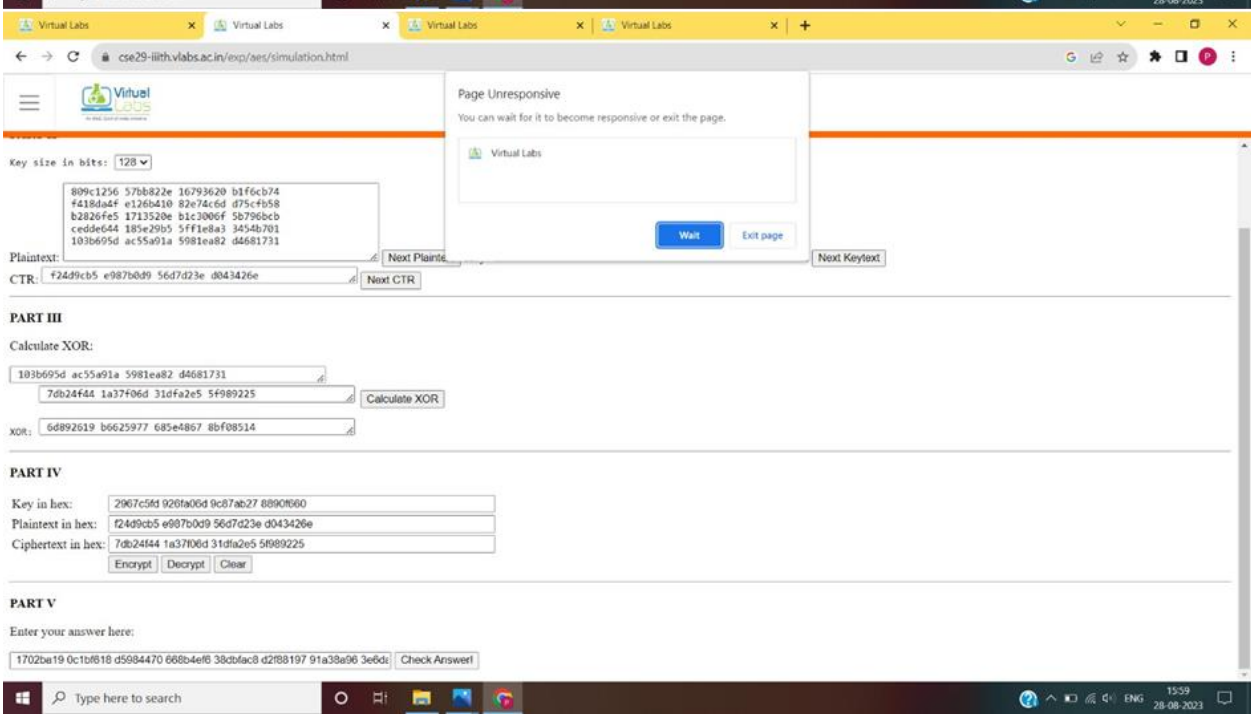

Virtual Labs
Virtual Labs
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
Virtual Labs
AES and Modes of Operation
Key size in bits: 128
efbfd9b5 16be4bf5 3f4a32ae 18225641
a28e6b05 f9dd6d0e 2ceb4ac6 43e0bcb0
4f4fda79 65b7567c bede510c 3feceea7
5b7befac 25904cc9 e8246988 e1c02e51
4f6a92c1 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!!
Type here to search
ENG
14:56
28-08-2023

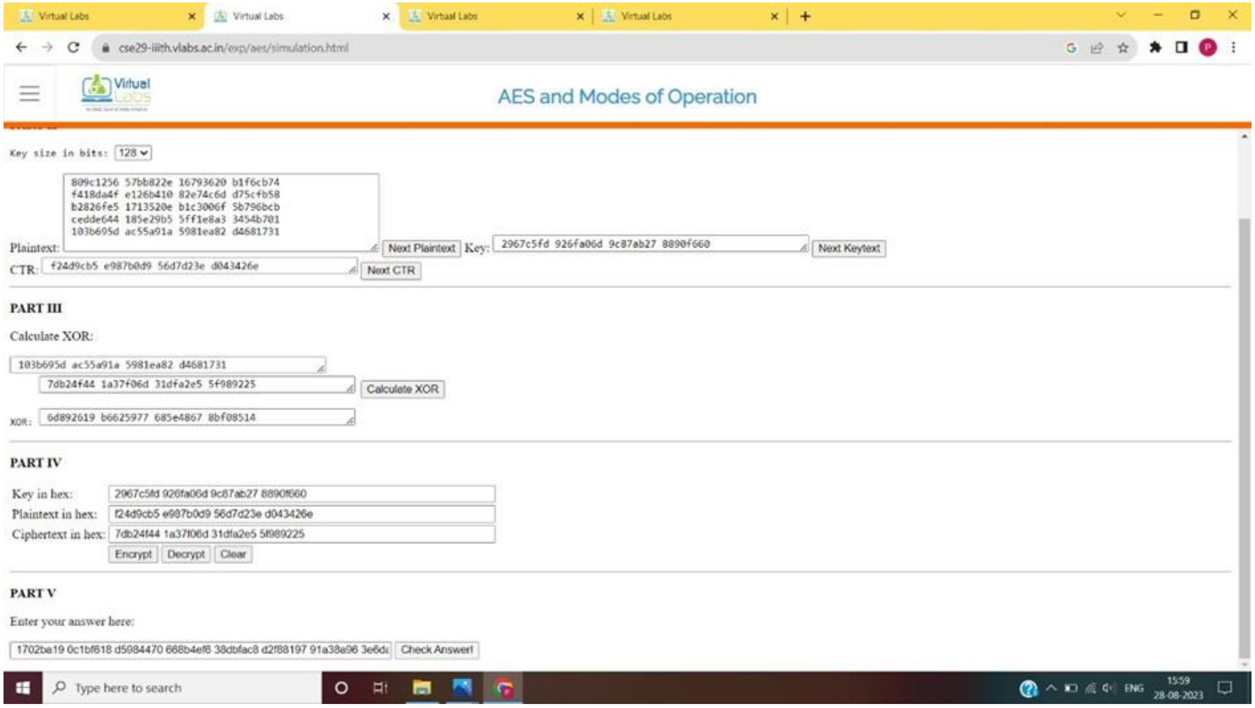

Virtual Labs
Virtual Labs
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
Virtual Labs
AES and Modes of Operation
PART I
Choose your mode of operation: Electronic Code Book (ECB)
PART II
Key size in bits: 128
9e02b6c4 6dad8409 a3dc592c 5f49e9c9
5ae4a86a 65c15647 f2b74f22 47dab354
21e25393 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
Type here to search
ENG
15:01
28-08-2023


Virtual Labs
Virtual Labs
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
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
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
15:01
28-08-2023


Virtual Labs
Virtual Labs
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
Virtual Labs
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
Type here to search
ENG
15:47
28-08-2023


AES and Modes of Operation
Plaintext:
c096db76 bc084d51 a0dc9fe9 b3e2f4b8
5eed2064 68029863 59b71c0c b06e91c1
66e3a8fd 4a183dc8 d2b75f18 dc305e0f
8c03d450 12880f54 03469256 ab884d88
67c2648a e98d960b 7e0110ac e8e31045
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:
Check Answer!
CORRECT!!


Page Unresponsive
You can wait for it to become responsive or exit the page.
Wait
Exit page
Key size in bits: 128
Plaintext:
809c1256 57bb822e 16793620 b1f6cb74
f418da4f e126b410 82e74c6d d75cfb58
b2826fe5 1713520e b1c3006f 5b796bcb
cedde644 185e29b5 5ff1e8a3 3454b701
103b695d ac55a91a 5981ea82 d4681731
CTR: f24d9cb5 e987b0d9 56d7d23e d043426e
Next CTR
Next Keytext
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:
Check Answer!



Conclusion:- Learnt about various modes of operation in block cipher such as ECB , CBC , OFB , CTR mode and also practically implemented them for randomly generated strings and performed AES on that string to get encrypted message