Animesh Parab T2-T21 88

ASSIGNMENT NO – 3

AIM: To understand AES cipher with various block cipher modes

LAB OUTCOME: LO2: Demonstrate Key Management, Distribution and Authentication.

THEORY:

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

☐ **AES (Advanced Encryption Standard)** is a symmetric-key block cipher that is widely used for secure data encryption. Here's a brief overview of its key characteristics along with an example:

1)Cipher Type: AES is a symmetric-key cipher, meaning the same key is used for both encryption and decryption.

2)Number of Rounds: The number of rounds in AES depends on the key size:

AES-128: 10 rounds

AES-192: 12 rounds

AES-256: 14 rounds

3)Key Size: AES supports three different key sizes: 128 bits (16 bytes), 192 bits (24 bytes), and 256 bits (32 bytes).

4)Block Size: AES processes data in fixed-size blocks of 128 bits (16 bytes). This means that data to be encrypted is divided into blocks, and each block is processed separately.

5)Operations in Each Round: Each round of AES consists of several operations:

a. **SubBytes:** Substitutes each byte in the block with a corresponding byte from a fixed S-box.

b. **ShiftRows:** Rearranges the bytes within each row of the block.

c. **MixColumns:** Mixes the columns within the block using a mathematical transformation.

d. **AddRoundKey:** XORs the block with a round-specific subkey derived from the original encryption key.

Example:

Let's encrypt a simple message "AES" using AES-128 with the key "EXAMPLEKEY12345." We'll perform one round of AES encryption:

Message: "AES"

Key: "EXAMPLEKEY12345" (128 bits)

Initial Round:

a. SubBytes: Replace each byte with a corresponding byte from the S-box.

Input: "AES"

Output (after substitution): "BDFA92"

b. ShiftRows: Rearrange bytes within rows (no change in the initial round).

c. MixColumns: Mix the columns within the block (not done in the initial round).

d. AddRoundKey: XOR the block with the first round key derived from the original key.

Initial Key: "EXAMPLEKEY12345"

Round 1 Key (derived from initial key): "375920614F761A3ECF4C1106D991F37F"

Input: "BDFA92"

Output (after XOR): "8863F2"

The encrypted message after one round is "8863F2." The remaining rounds are applied (9 more rounds for AES-128) to complete the encryption process.Decrypting the message involves reversing these steps with the same key and round keys in reverse order.

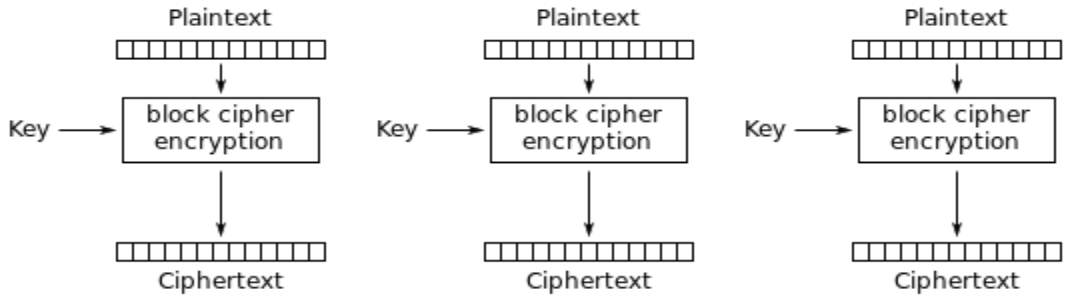
AES is a widely recognized and secure encryption standard used for protecting sensitive data in various applications, including secure communication, data storage, and more.

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

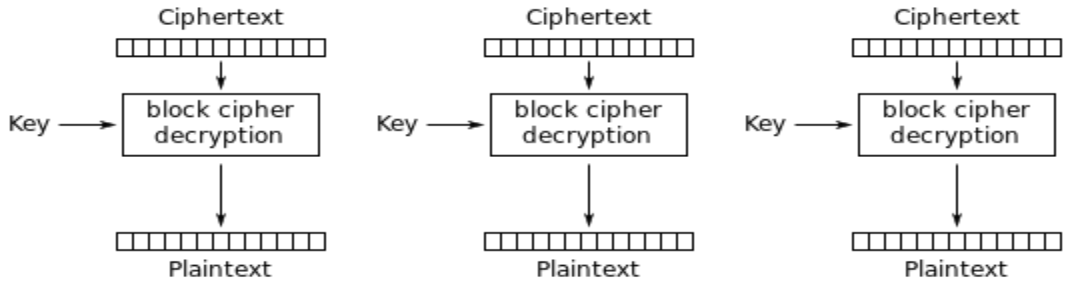
☐ Encryption algorithms are divided into two categories based on the input type, as a block cipher and stream cipher.

a)Electronic Code Book (ECB):–

Electronic code book is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of input plaintext and output is in form of blocks of encrypted ciphertext. Generally, if a message is larger than b bits in size, it can be broken down into a bunch of blocks and the procedure is repeated.



Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

Advantages of using ECB:–

- Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption.
- Simple way of the block cipher.

Disadvantages of using ECB:–

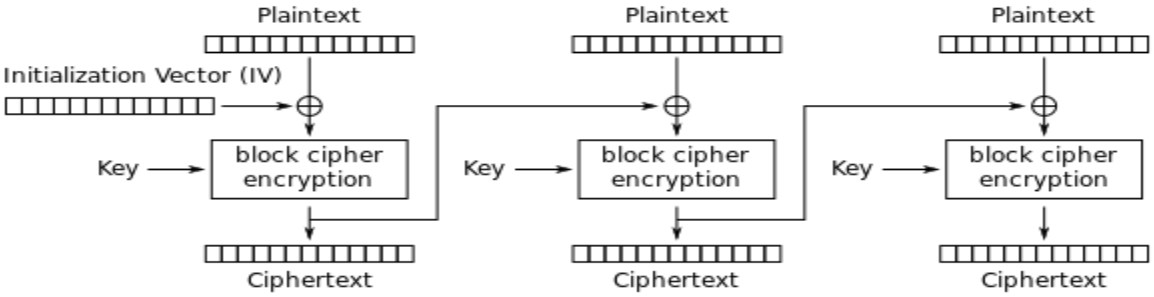
☐ Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext.

b)Cipher Block Chaining(CBC):–

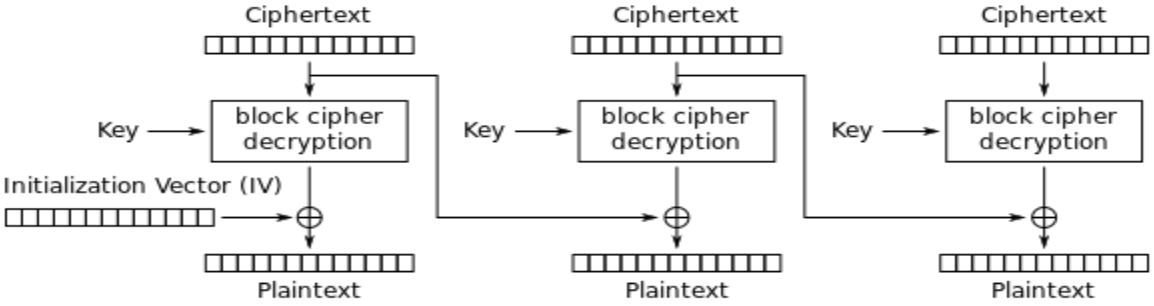
Cipher block chaining or CBC is an advancement made on ECB since ECB compromises some security requirements. In CBC, the previous cipher block is given as input to the

next encryption algorithm after XOR with the original plaintext block. In a nutshell here, a cipher block is produced by encrypting an XOR output of the previous cipher block and present plaintext block.

The process is illustrated here:



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Advantages of CBC:–

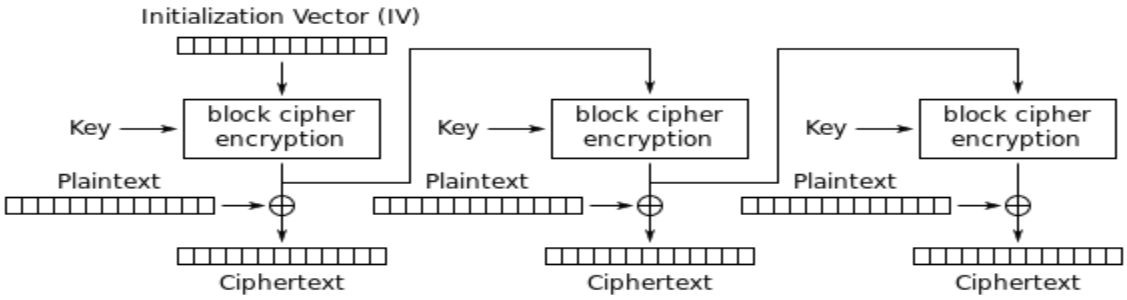
- CBC works well for input greater than b bits.
- CBC is a good authentication mechanism.
- Better resistive nature towards cryptanalysis than ECB.

Disadvantages of CBC:–

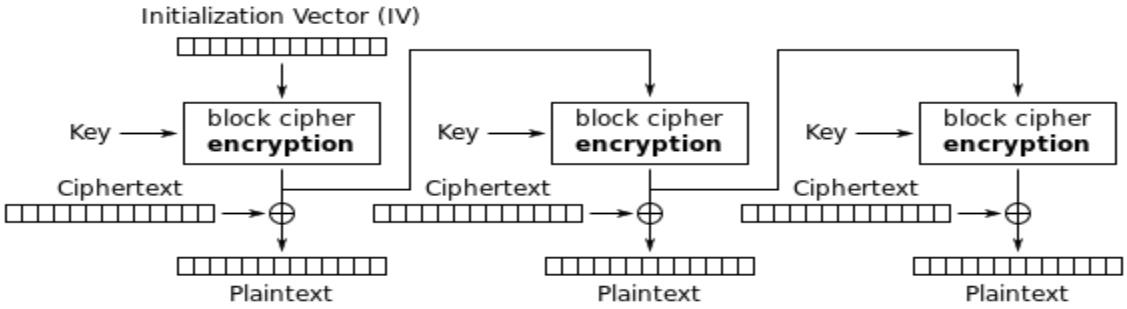
☐ Parallel encryption is not possible since every encryption requires a previous cipher.

c)Output Feedback Mode(OFB):–

The output feedback mode follows nearly the same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output. In this output feedback mode, all bits of the block are sent instead of sending selected s bits. The Output Feedback mode of block cipher holds great resistance towards bit transmission errors. It also decreases the dependency or relationship of the cipher on the plaintext.



Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption

Advantages of OFB:–

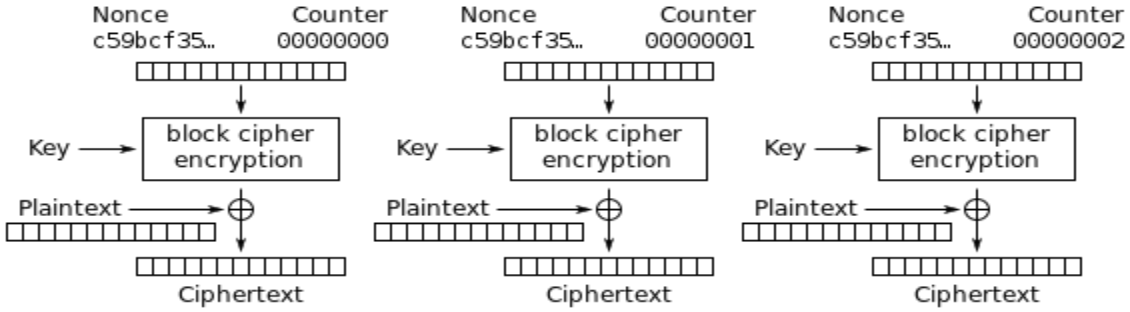
☐ In the case of CFB, a single bit error in a block is propagated to all subsequent blocks. This problem is solved by OFB as it is free from bit errors in the plaintext block.

Disadvantages of OFB:–

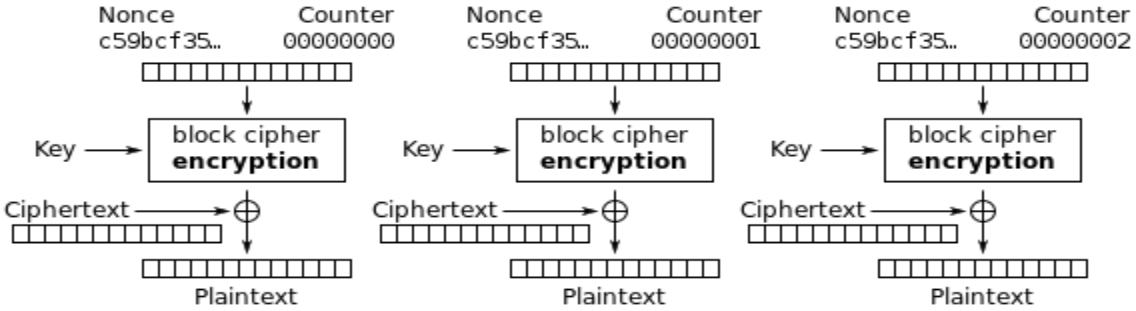
☐ The drawback of OFB is that, because to its operational modes, it is more susceptible to a message stream modiiccation attack than CFB. **d)Counter Mode:–**

The Counter Mode or CTR is a simple counter-based block cipher implementation. Every time a counter-initiated value is encrypted and given as input to XOR with plaintext which results in ciphertext block. The CTR mode is independent of feedback use and thus can be implemented in parallel.

Its simple implementation is shown below:



Counter (CTR) mode encryption



Counter (CTR) mode decryption

Advantages of Counter:–

- Since there is a different counter value for each block, the direct plaintext and ciphertext relationship is avoided. This means that the same plain text can map to different ciphertext.
- Parallel execution of encryption is possible as outputs from previous stages are not chained as in the case of CBC.

Disadvantages of Counter:-

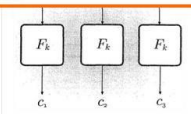
☐ The fact that CTR mode requires a synchronous counter at both the transmitter and the receiver is a severe drawback. The recovery of plaintext is erroneous when synchronisation is lost.

OUPUT FOR EVERY MODE:

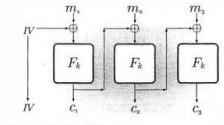
Activities Firefox Web Browser Tue 15:09

Virtual Labs | check answer in ecb in vi | https://cse29-iiith.vlabs.ac.in/exp/aes/theory.html 50%

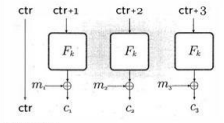
Assignment
References
Feedback



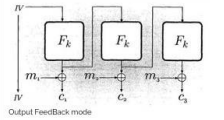
Electronic Code Book(ECB) mode



Cipher Block Chaining(CBC) mode



Contur mode



Output FeedBack mode

Community Links | Contact Us | Follow Us

Activities Firefox Web Browser Tue 15:08

Virtual Labs | check answer in ecb in vi | https://cse29-iiith.vlabs.ac.in/exp/aes/simulation.html 80%

AES and Modes of Operation

PART I

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

PART II

Key size in bits: 128

Plaintext: 789dd094 1ed35c5a 38d6d4c7 75697125
feea1f33 af3ba572 777db0d1 79139fd1
52930f25 70d74f6a 87e0105b b8f3cdf5
526f05e8 859547d0 faac25a9 d1c522f4
f8ba699b 569815ed 66a49d3d 7b53d172

Next Plaintext Key: 2f57afd1 2738c036 3ddf8695 85802789 Next Keytext

IV: Next IV

CTR: Next CTR

PART III

Calculate XOR:

Calculate XOR

XOR:

PART IV

Key in hex: 2f57afd1 2738c036 3ddf8695 85802789

Plaintext in hex: f8ba699b 569815ed 66a49d3d 7b53d172

Ciphertext in hex: 3e6c556b 9cd03380 48b0e055 79ab7a2c

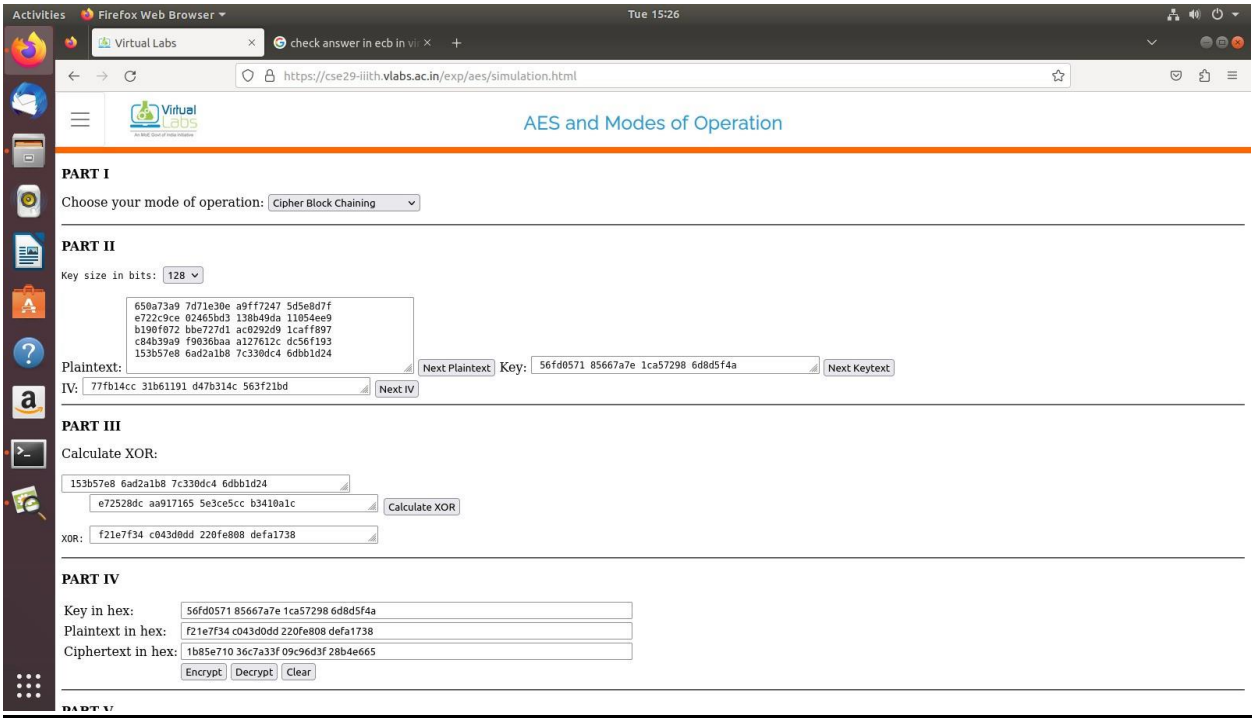
Encrypt Decrypt Clear

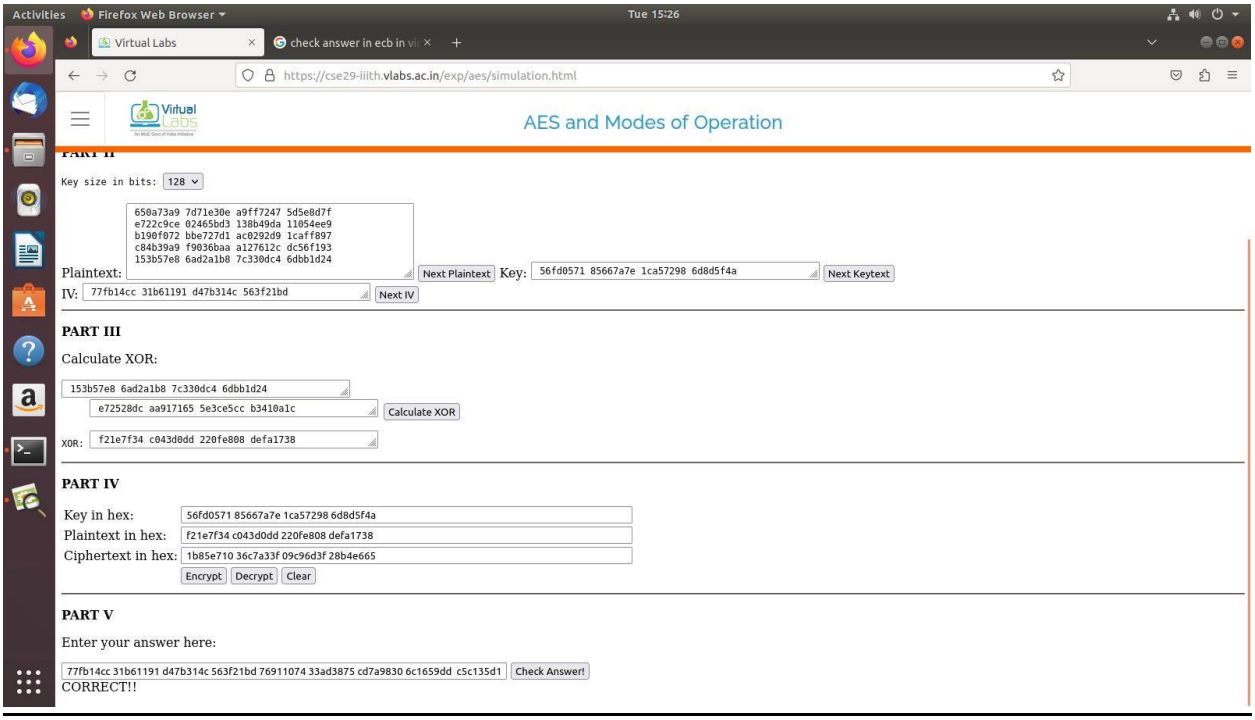
PART V

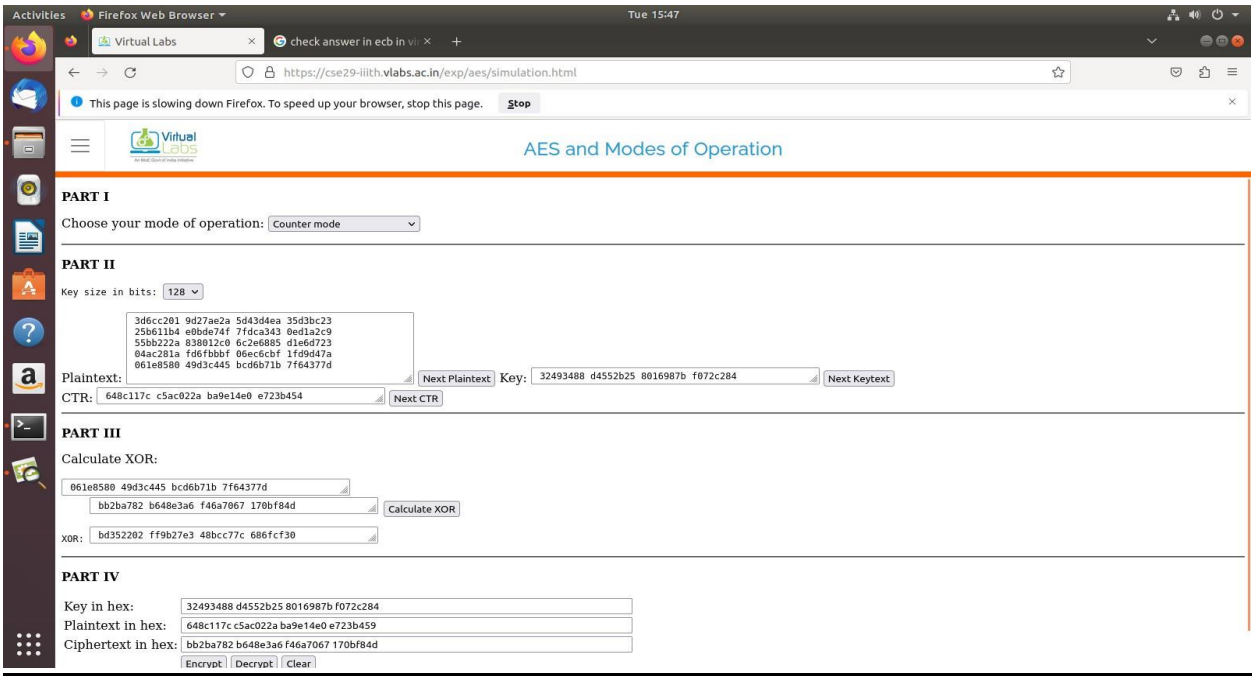
Enter your answer here:

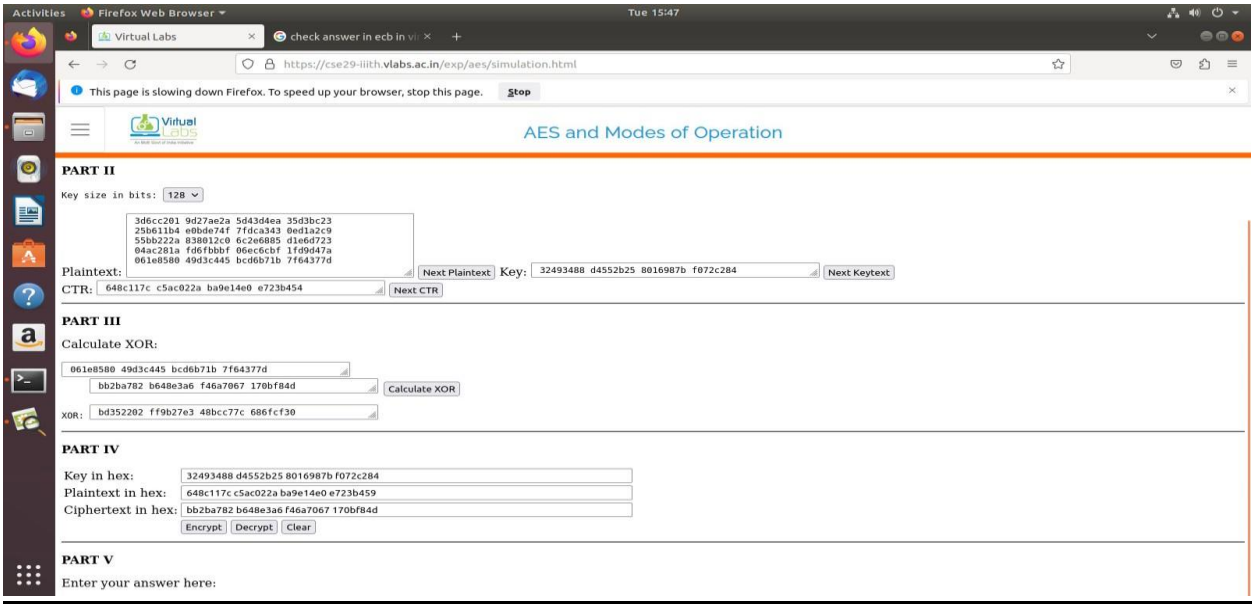
14bca2b 45bc5adc 12f7b066 6e93ffd5 fc43c89a a5893c99 3e6c556b 9cd03380 48b0e0 Check Answer!

CORRECT!!


Activities
Firefox Web Browser
Tue 15:26
Virtual Labs
check answer in ecb in vi
https://cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
AES and Modes of Operation
PART I
Choose your mode of operation: Cipher Block Chaining
PART II
Key size in bits: 128
650a73a9 7d71e30e a9ff7247 5d5e8d7f
e722c9ce 02465bd3 138b49da 11054ee9
b190f072 bbe727d1 ac0292d9 1caff897
c84b39a9 f9036baa a127612c dc56f193
153b57e8 6ad2a1b8 7c330dc4 6dbb1d24
Plaintext:
Next Plaintext
Key: 56fd0571 85667a7e 1ca57298 6d8d5f4a
Next Keytext
IV: 77fb14cc 31b61191 d47b314c 563f21bd
Next IV
PART III
Calculate XOR:
153b57e8 6ad2a1b8 7c330dc4 6dbb1d24
e72528dc aa917165 5e3ce5cc b3410a1c
Calculate XOR
XOR: f21e7f34 c043d0dd 220fe808 defa1738
PART IV
Key in hex: 56fd0571 85667a7e 1ca57298 6d8d5f4a
Plaintext in hex: f21e7f34 c043d0dd 220fe808 defa1738
Ciphertext in hex: 1b85e710 36c7a33f 09c96d3f 28b4e665
Encrypt
Decrypt
Clear


Activities
Firefox Web Browser
Tue 15:26
Virtual Labs
check answer in ecb in vi
https://cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
AES and Modes of Operation
Key size in bits: 128
650a73a9 7d71e30e a9ff7247 5d5e8d7f
e722c9ce 02465bd3 138b49da 11054ee9
b190f072 bbe727d1 ac0292d9 1caff897
c84b39a9 f9036baa a127612c dc56f193
153b57e8 6ad2a1b8 7c330dc4 6dbb1d24
Plaintext:
Next Plaintext
Key: 56fd0571 85667a7e 1ca57298 6d8d5f4a
Next Keytext
IV: 77fb14cc 31b61191 d47b314c 563f21bd
Next IV
PART III
Calculate XOR:
153b57e8 6ad2a1b8 7c330dc4 6dbb1d24
e72528dc aa917165 5e3ce5cc b3410a1c
Calculate XOR
XOR: f21e7f34 c043d0dd 220fe808 defa1738
PART IV
Key in hex: 56fd0571 85667a7e 1ca57298 6d8d5f4a
Plaintext in hex: f21e7f34 c043d0dd 220fe808 defa1738
Ciphertext in hex: 1b85e710 36c7a33f 09c96d3f 28b4e665
Encrypt
Decrypt
Clear
PART V
Enter your answer here:
77fb14cc 31b61191 d47b314c 563f21bd 76911074 33ad3875 cd7a9830 6c1659dd c5c135d1
Check Answer!
CORRECT!!





CONCLUSION: Successfully, we learnt utilizing the AES cipher with various block cipher modes, it is crucial to carefully evaluate the speciicc security and operational requirements. Always implement the chosen mode correctly and adhere to best practices to uphold the security of your data.