Roll No: 09
Name: Shreya Bagade
Date: 18/08/2023

LAB ASSIGNMENT NO:03

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

Lab Outcome Attained: 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. AES operates on fixed-size blocks of data and employs a substitution-permutation network (SPN) structure. It was selected by the National Institute of Standards and Technology (NIST) as the encryption standard in 2001, replacing the older Data Encryption Standard (DES).

Number of Rounds: AES operates with different numbers of rounds based on the key size:

128-bit key: 10 rounds

192-bit key: 12 rounds

256-bit key: 14 rounds

Key Size: AES supports key sizes of 128, 192, and 256 bits.

Block Size: AES operates on blocks of data, and the block size for AES is fixed at 128 bits.

Operations in Each Round:

SubBytes: Byte substitution using a fixed substitution table (S-box). Each byte in the block is replaced with a corresponding byte from the S-box.

ShiftRows: Byte shifting within rows of the block. The first row remains unchanged, the second row shifts by one byte to the left, the third row shifts by two bytes, and the fourth row shifts by three bytes.

MixColumns: Column-wise mixing operation. Each column is treated as a polynomial and is transformed through a matrix multiplication operation. This step provides diffusion and helps achieve confusion.

AddRoundKey: A bitwise XOR operation where each byte of the block is combined with the corresponding byte of the round key. The round key is derived from the original encryption key using a key expansion algorithm.

These operations are performed for the specified number of rounds based on the key size. The additional security of AES stems from its key expansion algorithm, which generates a set of round keys from the original encryption key. Each round key is used in the AddRoundKey step, adding a layer of complexity and security.

Overall, AES is a highly secure and efficient encryption algorithm that offers strong protection for sensitive data. Its adoption as a standard encryption mechanism in various applications demonstrates its robustness and reliability.

> With diagram explain in brief block cipher modes of operation

1. ECB mode
2. CBC mode
3. OFB mode
4. Counter mode

A block cipher processes the data blocks of fixed size. Usually, the size of a message is larger than the block size. Hence, the long message is divided into a series of sequential message blocks, and the cipher operates on these blocks one at a time.

Electronic Code Book (ECB) Mode

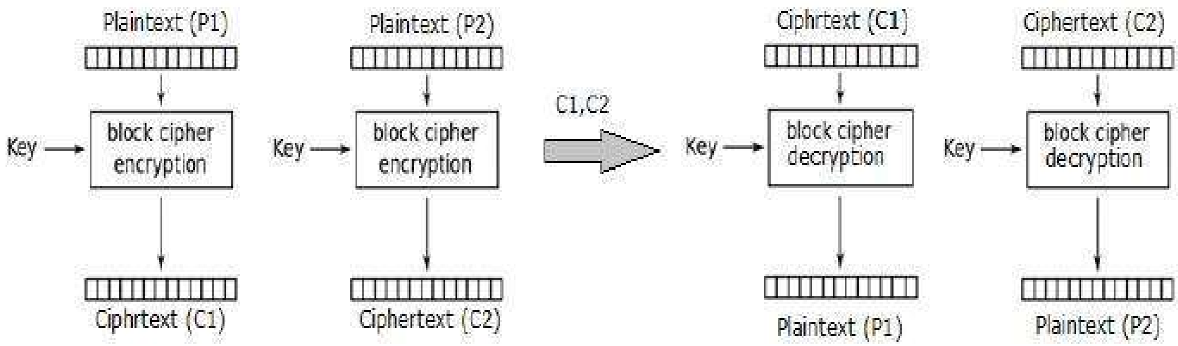
This mode is a most straightforward way of processing a series of sequentially listed message blocks.

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 −



<u>Analysis of ECB Mode</u>

In reality, any application data usually have partial information which can be guessed. For example, the range of salary can be guessed. A ciphertext from ECB can allow an attacker to guess the plaintext by trial-and-error if the plaintext message is within predictable.

For example, if a ciphertext from the ECB mode is known to encrypt a salary figure, then a small number of trials will allow an attacker to recover the figure. In general, we do not wish to use a deterministic cipher, and hence the ECB mode should not be used in most applications.

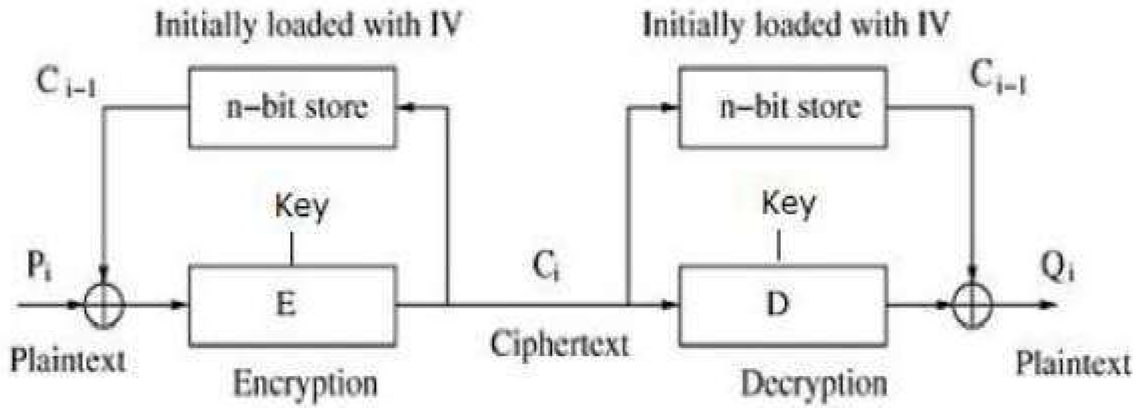
Cipher Block Chaining (CBC) Mode

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.



<u>Analysis of CBC Mode</u>

In CBC mode, the current plaintext block is added to the previous ciphertext block, and then the result is encrypted with the key. Decryption is thus the reverse process, which involves decrypting the current ciphertext and then adding the previous ciphertext block to the result.

Advantage of CBC over ECB is that changing IV results in different ciphertext for identical message. On the drawback side, the error in transmission gets propagated to few further block during decryption due to chaining effect.

It is worth mentioning that CBC mode forms the basis for a well-known data origin authentication mechanism. Thus, it has an advantage for those applications that require both symmetric encryption and data origin authentication.

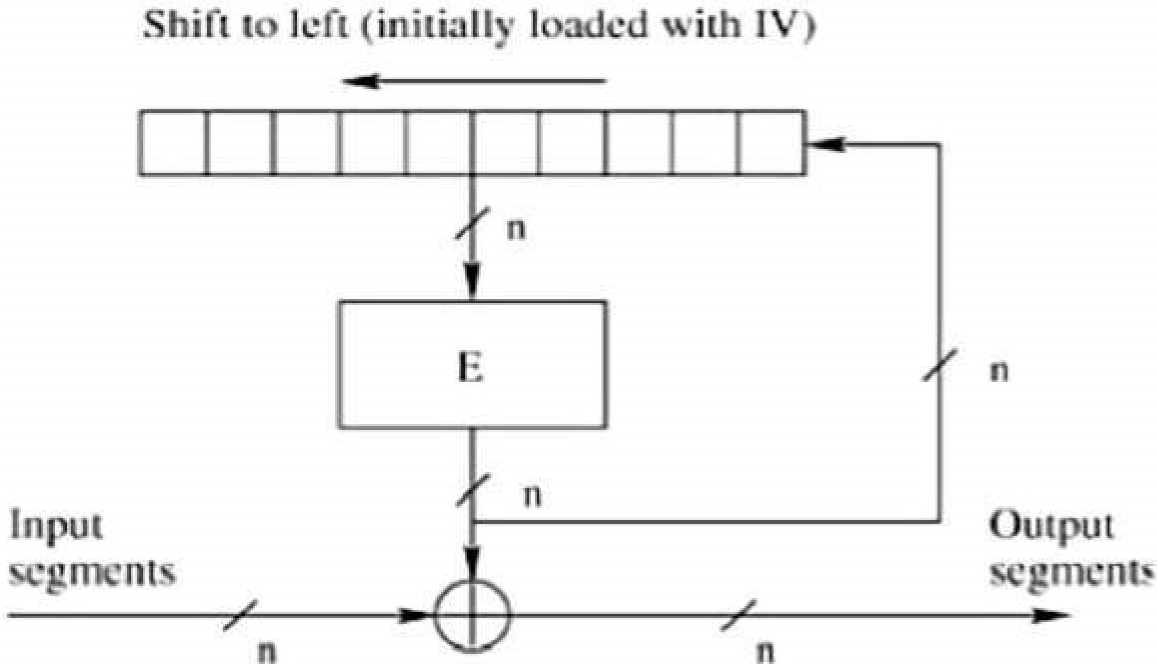
Output Feedback (OFB) Mode

It involves feeding the successive output blocks from the underlying block cipher back to it. These feedback blocks provide string of bits to feed the encryption algorithm which act as the key-stream generator as in case of CFB mode.

The key stream generated is XOR-ed with the plaintext blocks. The OFB mode requires an IV as the initial random n-bit input block. The IV need not be secret.

The operation is depicted in the following illustration −

Roll No: 09
Name: Shreya Bagade
Date: 18/08/2023



Counter (CTR) Mode

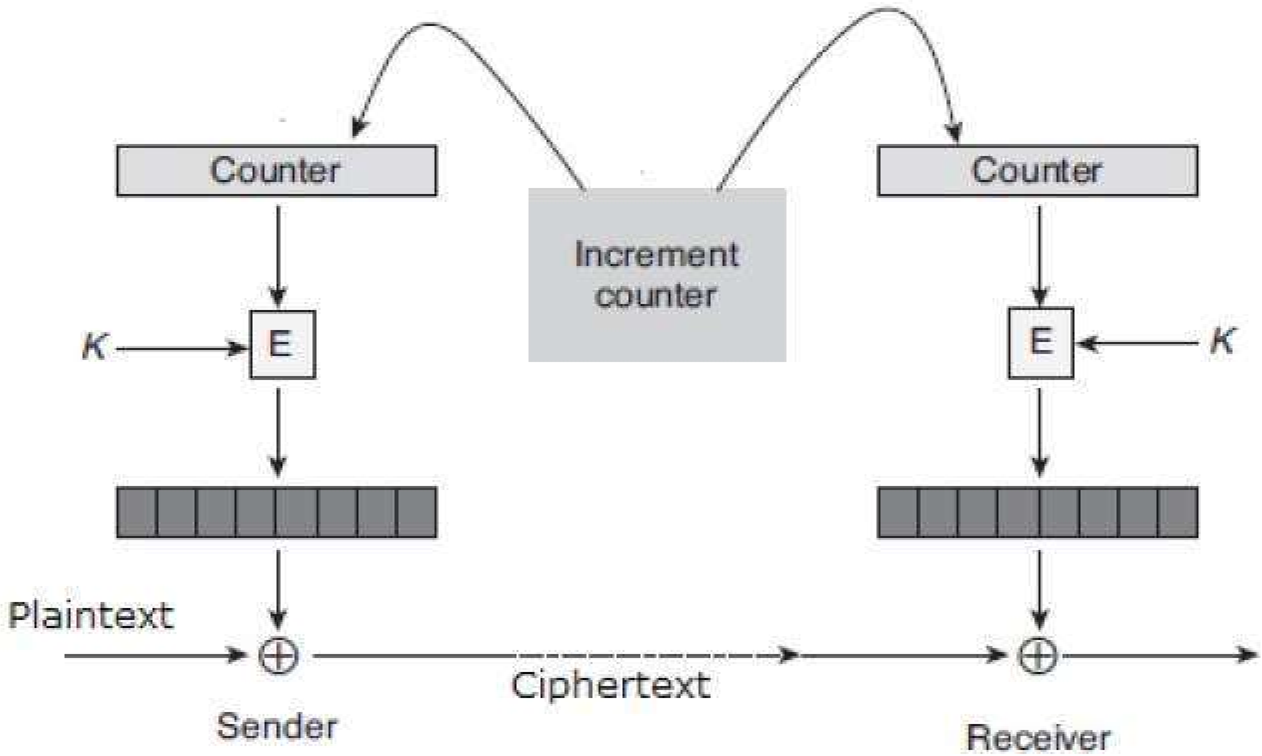
It can be considered as a counter-based version of CFB mode without the feedback. In this mode, both the sender and receiver need to access to a reliable counter, which computes a new shared value each time a ciphertext block is exchanged. This shared counter is not necessarily a secret value, but challenge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

Roll No: 09
Name: Shreya Bagade
Date: 18/08/2023



Analysis of Counter Mode

It does not have message dependency and hence a ciphertext block does not depend on the previous plaintext blocks.

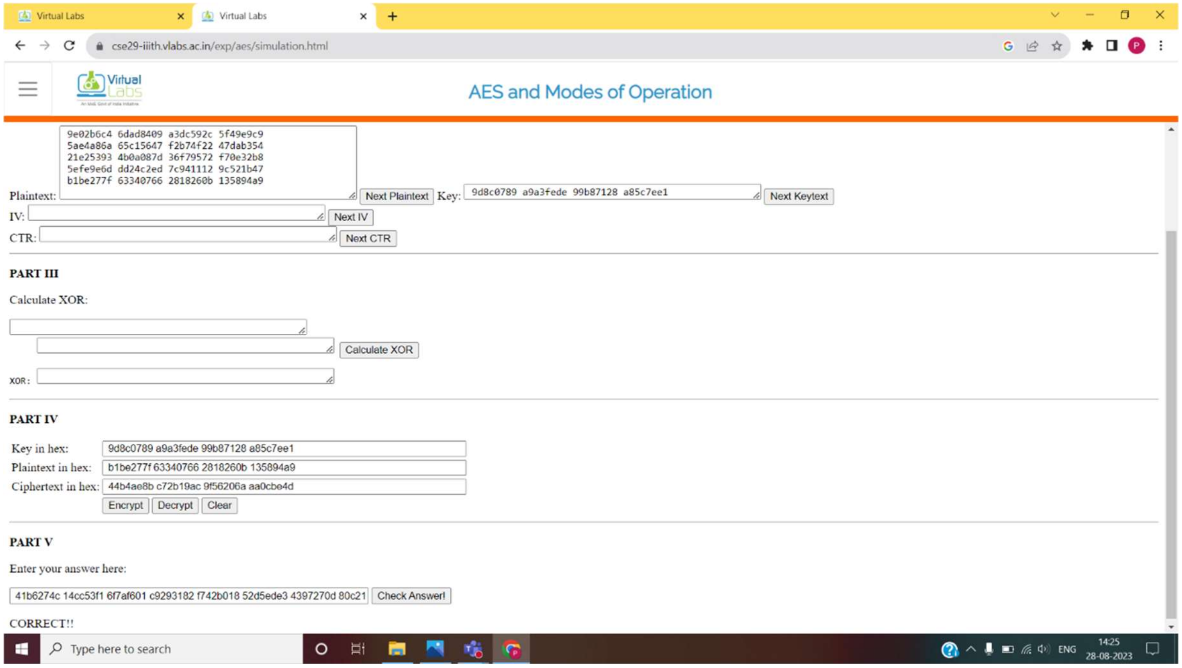
Like CFB mode, CTR mode does not involve the decryption process of the block cipher. This is because the CTR mode is really using the block cipher to generate a key-stream, which is encrypted using the XOR function. In other words, CTR mode also converts a block cipher to a stream cipher.

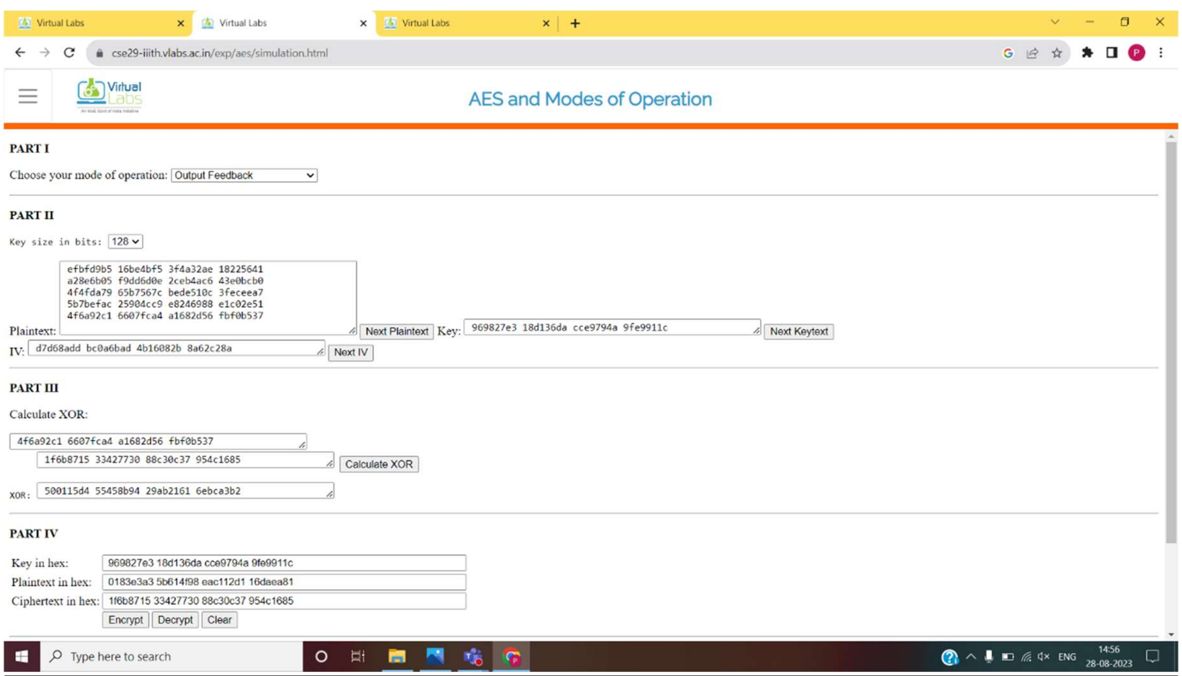
The serious disadvantage of CTR mode is that it requires a synchronous counter at sender and receiver. Loss of synchronization leads to incorrect recovery of plaintext.

However, CTR mode has almost all advantages of CFB mode. In addition, it does not propagate error of transmission at all.

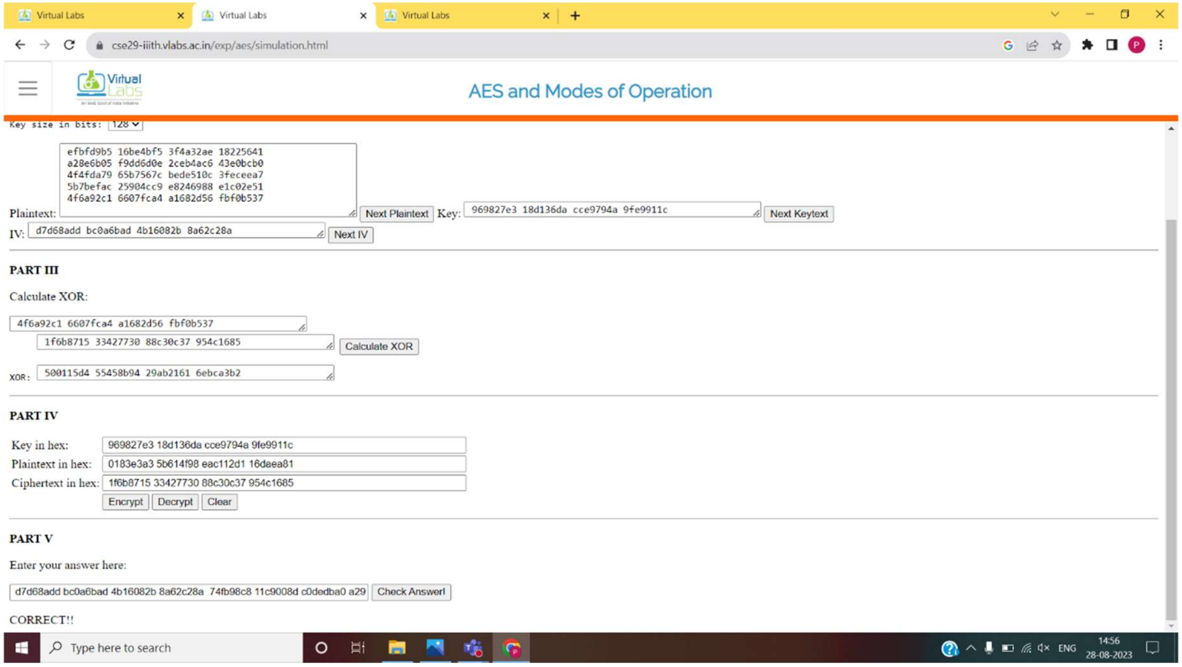
Roll No: 09
Name: Shreya Bagade
Date: 18/08/2023

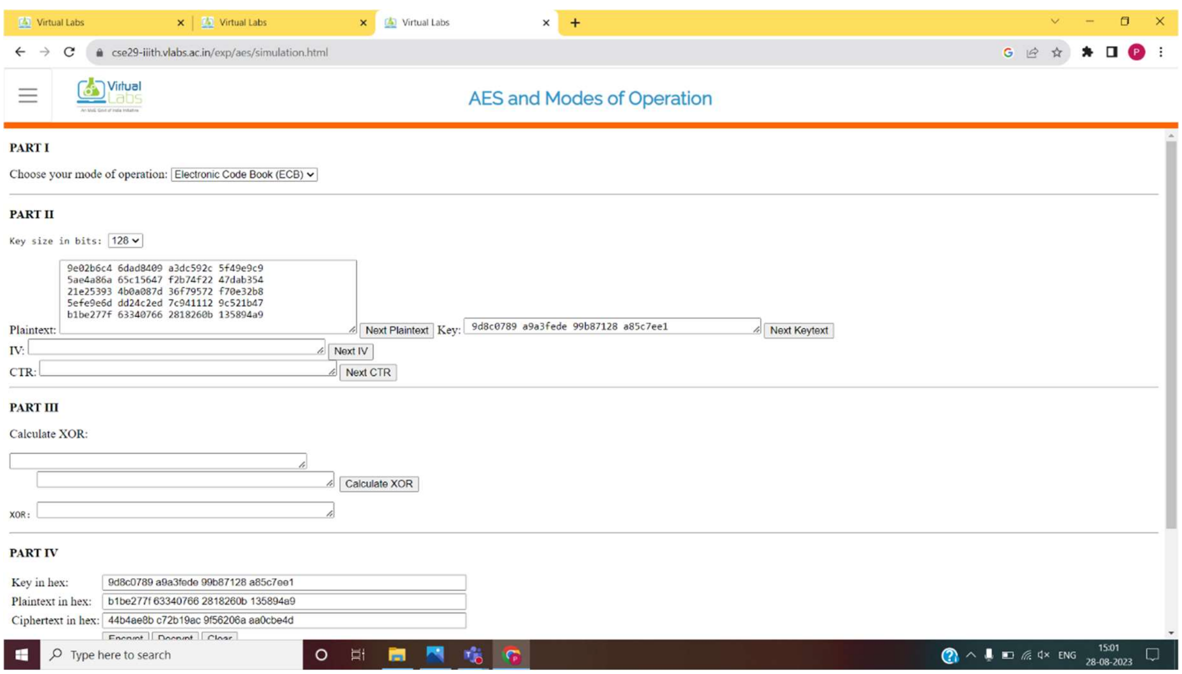
Output Screenshots:



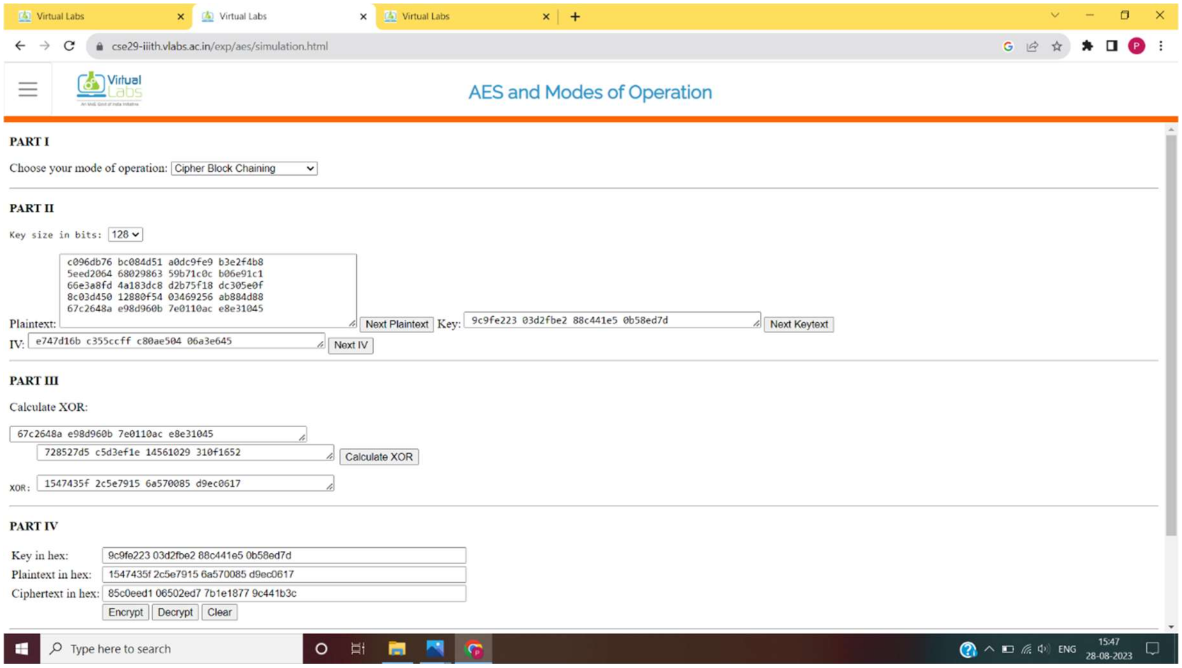


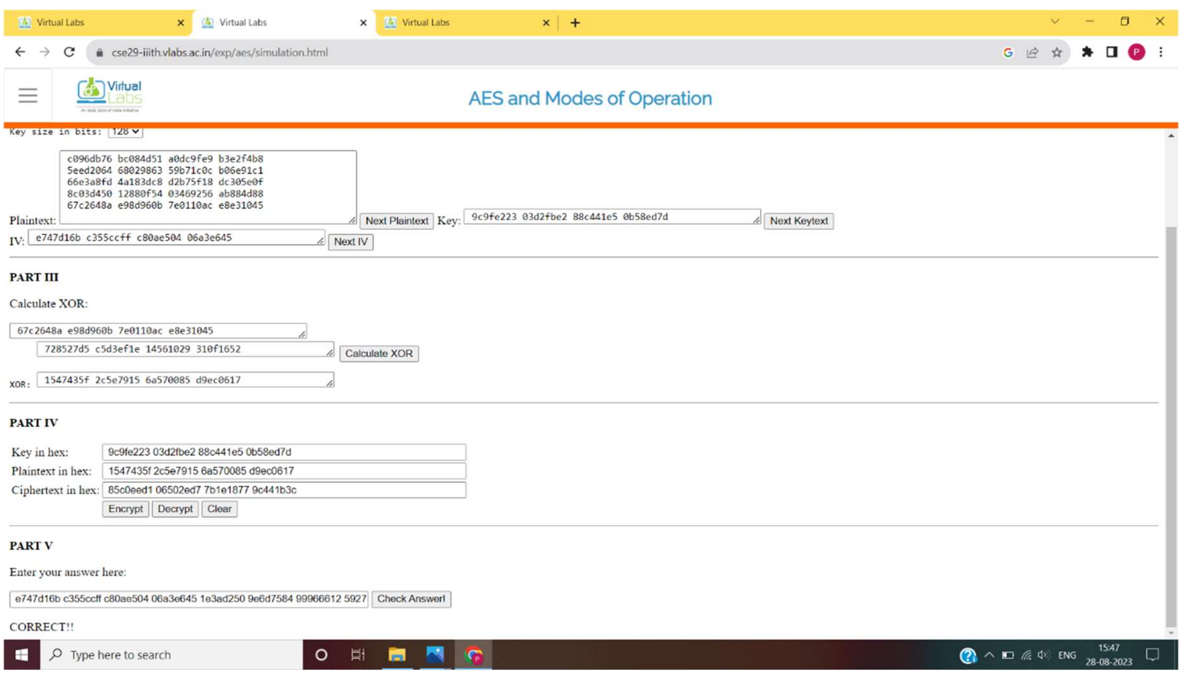
Roll No: 09
Name: Shreya Bagade
Date: 18/08/2023



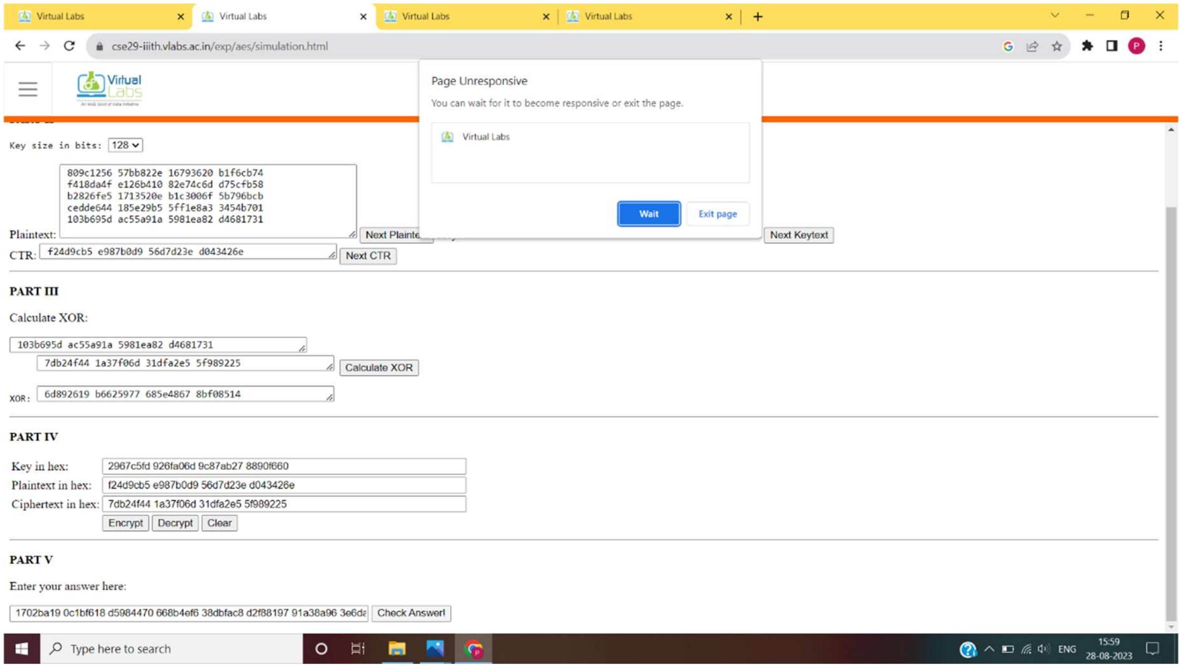


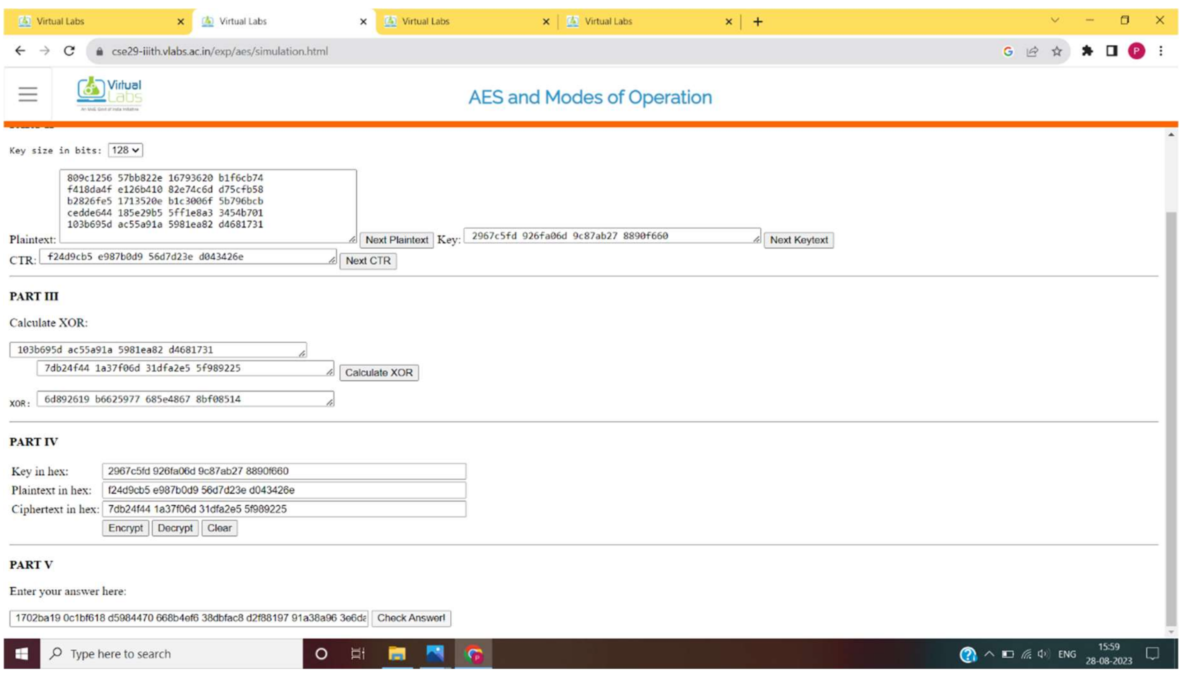
Roll No: 09
Name: Shreya Bagade
Date: 18/08/2023





Roll No: 09
Name: Shreya Bagade
Date: 18/08/2023





Conclusion: This experiment focused on the study of the Advanced Encryption Standard (AES) algorithm and its application in Cipher Block Chaining (CBC) mode has provided valuable insights into modern symmetric encryption techniques. Through this experiment, we gained a deeper understanding of how AES operates and how different modes of operation, such as CBC, contribute to enhancing security and confidentiality.