Experiment 05

To understand how to Encrypt long messages using various modes of operation using AES

Roll No.	14
Name	Ishika Sanjay Devare
Class	D15-A
Subject	Security Lab
LO Mapped	LO1: To apply the knowledge of symmetric cryptography to implement classical ciphers.

Aim: To Encrypt long messages using various modes of operation using AES.

Introduction:

AES stands for Advanced Encryption Standard and is a symmetric encryption algorithm. It is mainly used for encryption and protection of electronic data. It was used as the replacement of DES(Data Encryption Standard) as it is much faster and better than DES. AES consists of three block ciphers that are used to provide encryption of data.

History:

AES was developed by NIST(National Institute of Standard and Technology) in 1997. It was developed to replace DES which was slow and vulnerable to various attacks. So, therefore a new encryption algorithm was made to overcome the shortcomings of DES. AES was published on 26th November 2001.

Characteristics:

- AES has keys of three lengths which are 128, 192, 256 bits.
- It is flexible and has implementations for software and hardware.
- It provides high security and can prevent many attacks.
- It doesn't have any copyright so it can be easily used globally
- It consists of 10 rounds of processing for 128-bit keys.

Advantages:

It can be implemented on both hardware and software.
It provides high security to the users.
It provides one of the best open source solutions for encryption.
It is a very robust algorithm.

Disadvantages:

It requires many rounds for encryption.
It is hard to implement on software.
It needs much processing at different stages.
It is difficult to implement when performance has to be considered.

Block Cipher modes of Operation:

Encryption algorithms are divided into two categories based on input type, as block cipher and stream cipher. Block Cipher algorithm is an encryption algorithm which takes fixed size of input i.e b bits and produces a ciphertext of b bits again. If input is larger than b bits it can be divided further. For different applications and uses, there are several nodes of operations for a block cipher.

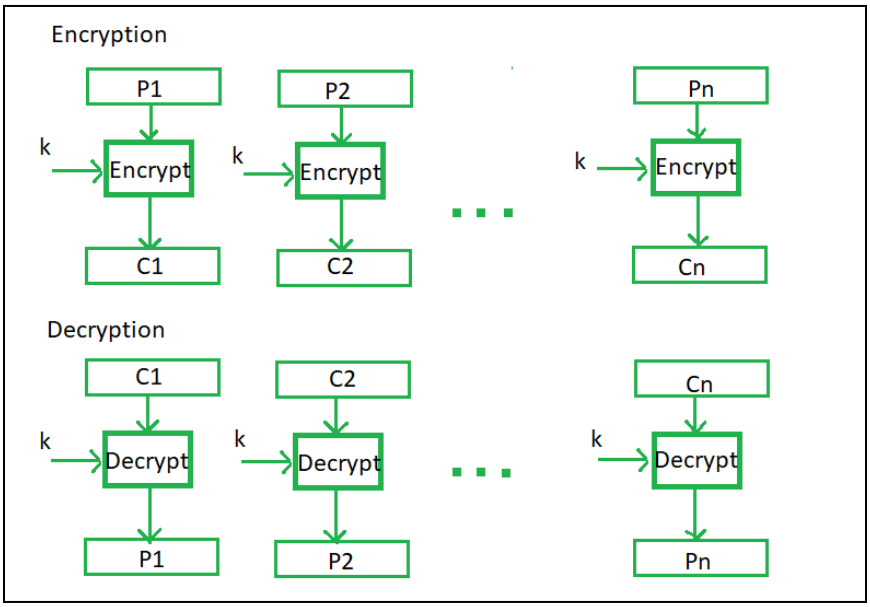
Methods are:

Different methods of Block Cipher mode of Operation are:

1. **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 the 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.

   Procedure of ECB is illustrated as-



Advantages:

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

Disadvantages:

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

Applications:

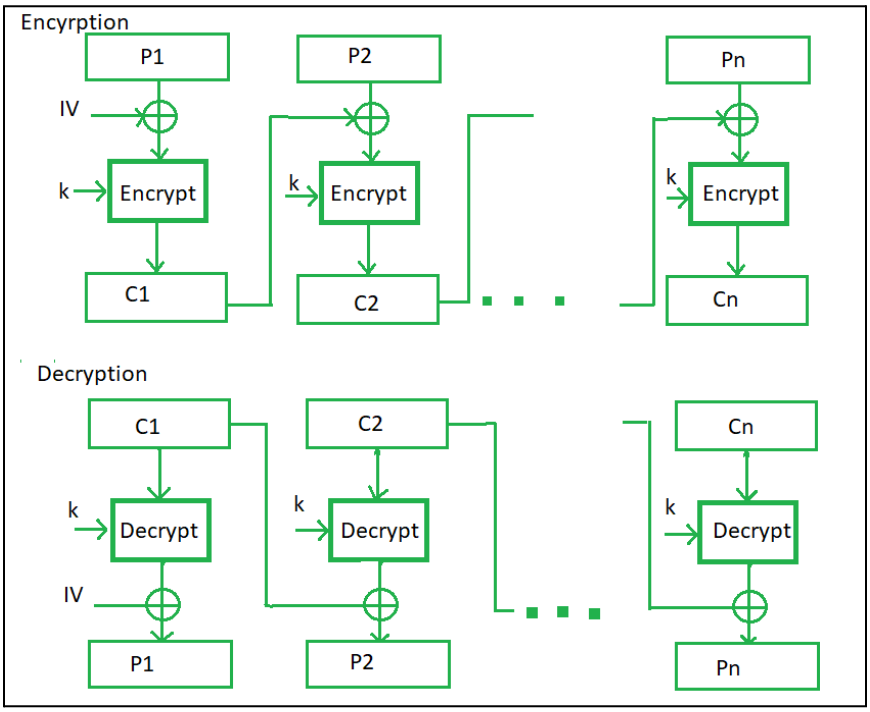
1. If a message is short enough to fit in one block, security issues and error propagation are tolerable.
2. It is useful where records need to be encrypted before they are stored in a database.

3. ECB allows parallel processing, if we want to create a very huge encrypted database.

2. **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.

Procedure of CBC is illustrated as-



Advantages:

1. Cipher Block Chaining works well for input greater than b bits.
2. CBC is a good authentication mechanism.
3. Better resistive nature towards cryptanalysis than ECB.

Disadvantages:

1. Parallel encryption is not possible as every encryption requires a previous cipher.

Application:

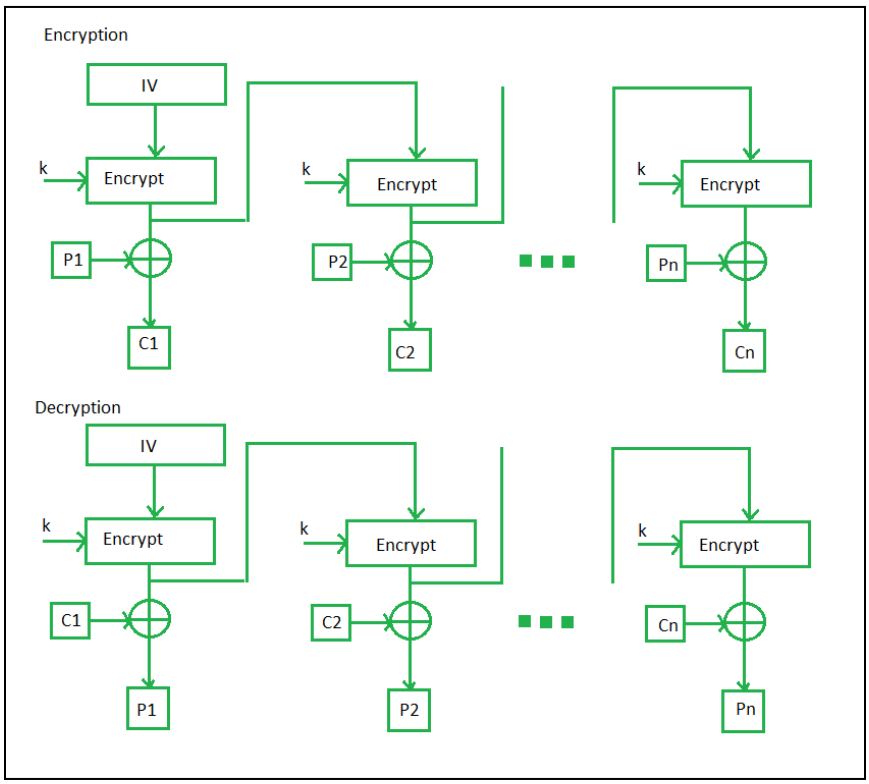
1. It is not used when we need parallel processing because it uses a chaining mechanism.

2. It is not used to encrypt and decrypt random-access files because encipherment here requires access to previous records.
3. It is used for authentication purposes.

3. Output Feedback Mode:

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.

Procedure of OFB is illustrated as-



Advantages:

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:

OFB is more vulnerable to a message stream modification attack than is CFB in the modes of operation.

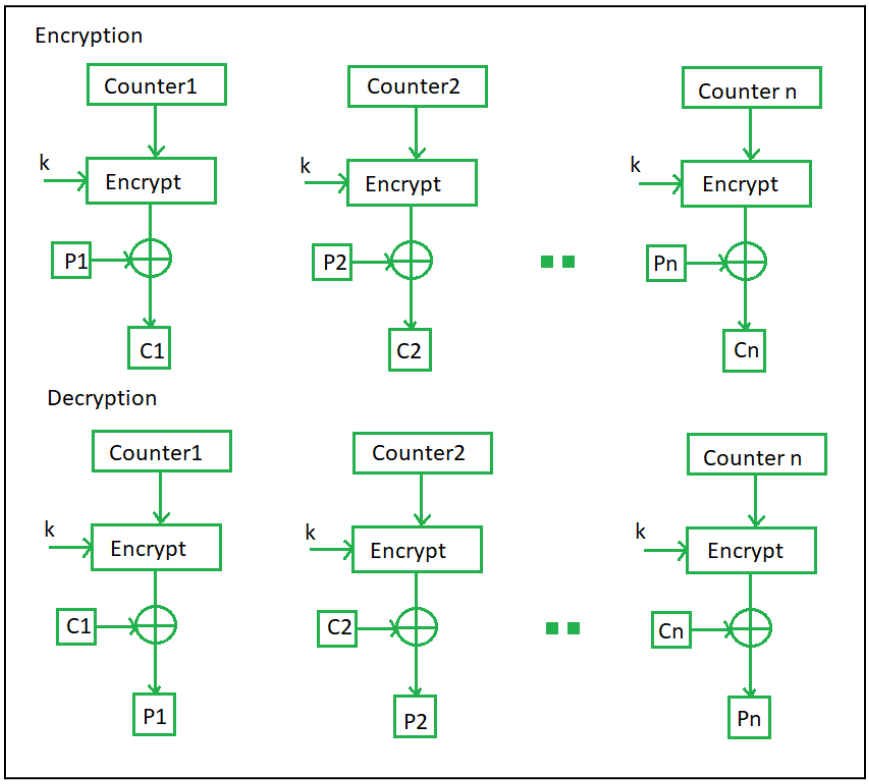
Applications:

Can be used to encipher blocks of small size such as one character or bit at a time. No need for padding because the size of the plaintext block is normally fixed.

4. **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 a ciphertext block. The CTR mode is independent of feedback use and thus can be implemented in parallel.

Procedure of Counter Mode is illustrated as-



Advantages:

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

Disadvantages:

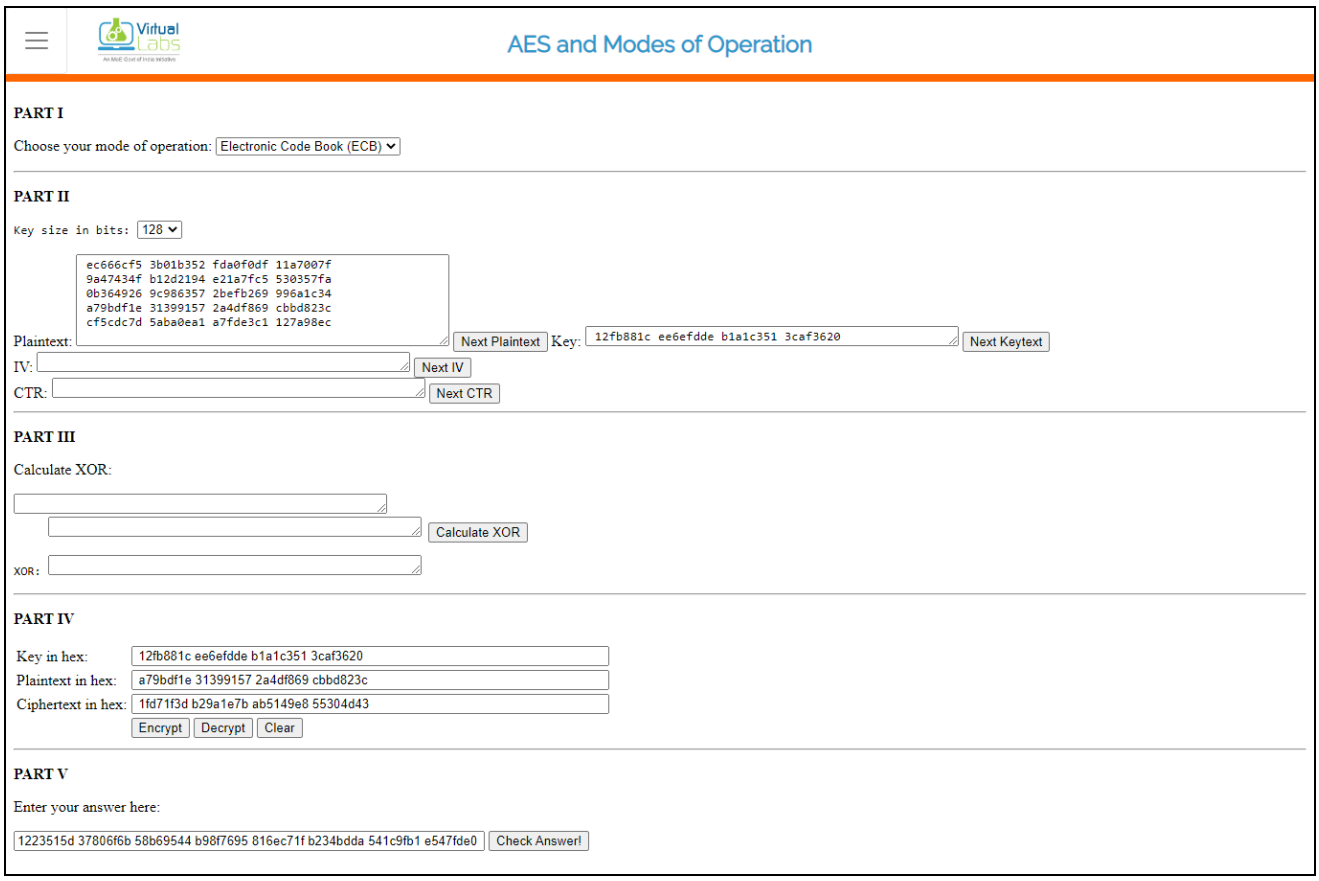
1. It requires a synchronous counter at the sender and receiver in this mode. Decreases of synchronization lead to incorrect recovery of plaintext or original text.

What is Vlab?

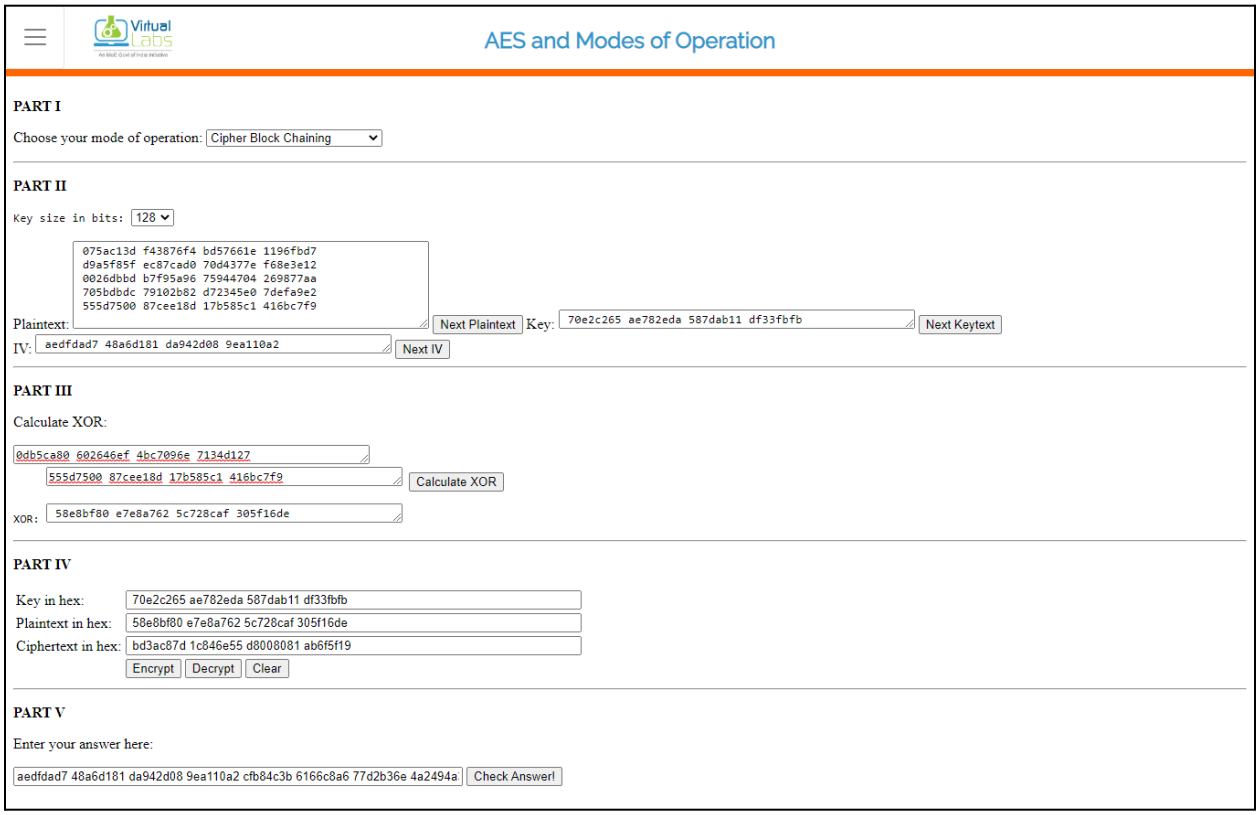
It provides remote-access to simulation-based Labs in various disciplines of Science and Engineering.

Results:

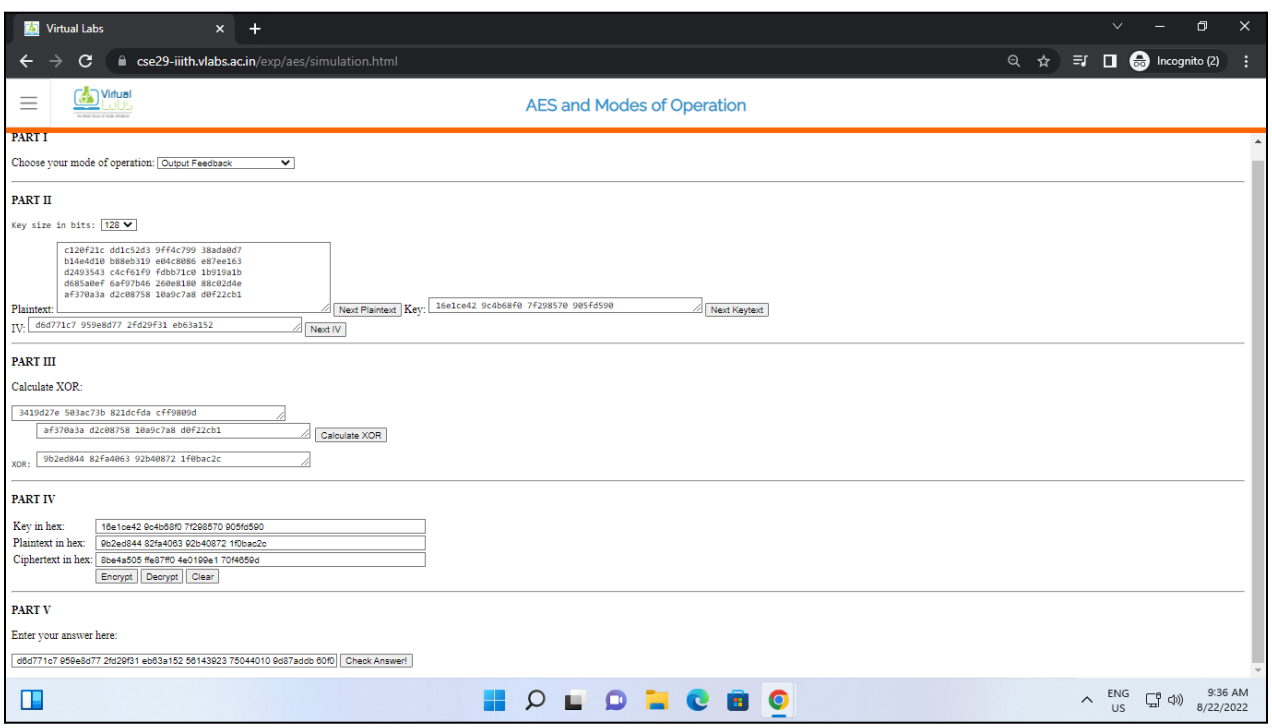
1. Electronic Code Book (ECB)



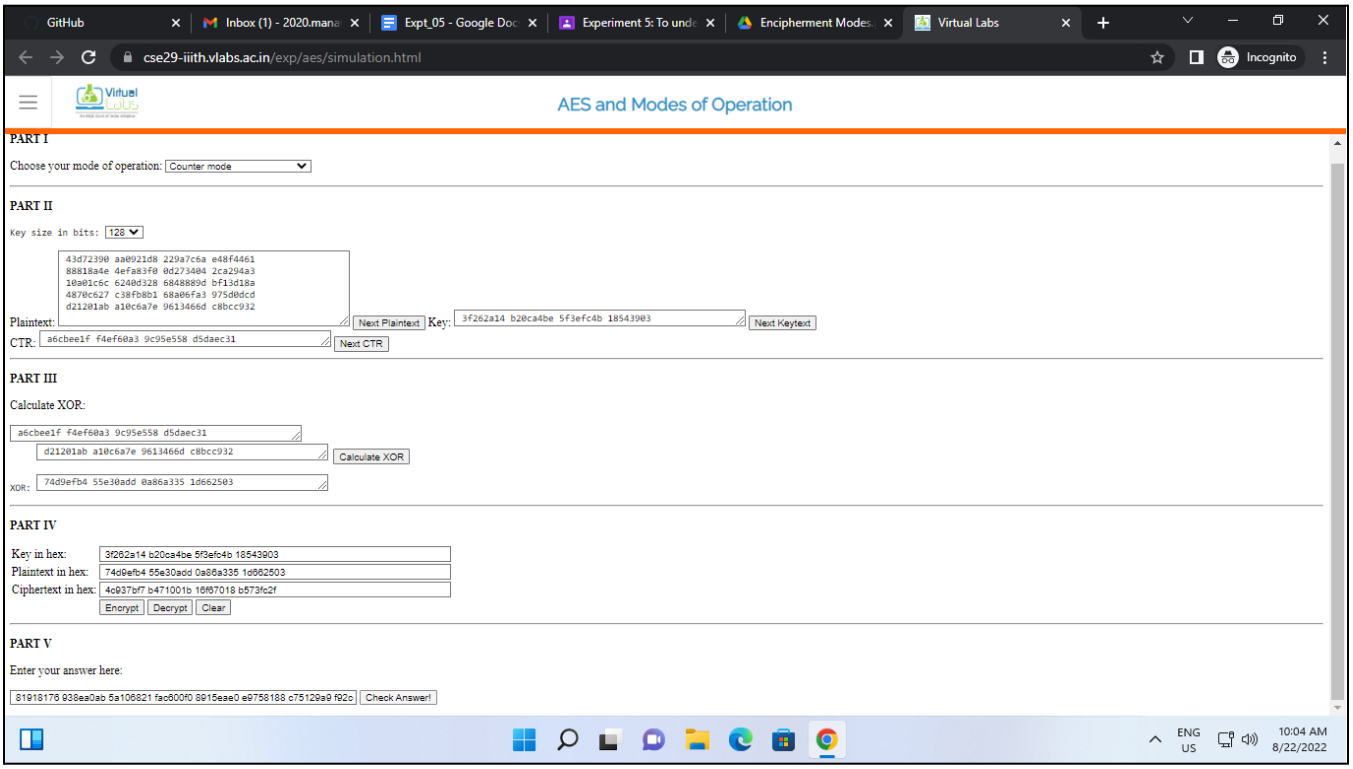
2. Cipher Block Chaining



3. Output Feedback



4. Counter Mode



Conclusion: Hence, we successfully understood how to Encrypt long messages using various modes of operation using AES.