Experiment 05

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

Roll No.	19
Name	Manav Jawrani
Class	D15-A
Subject	Security Lab
LO Mapped	LO1: To apply the knowledge of symmetric cryptography to implement classical ciphers.

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

Introduction:

AES algorithm:

AES stands for Advanced Encryption Standard and is a majorly used 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 and these ciphers are used to provide encryption of data.

Block Cipher modes of Operation:

Encryption algorithms are divided into two categories based on input type, as block cipher and stream cipher. Block cipher is an encryption algorithm which takes fixed size of input, say 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 modes of operations for a block cipher.

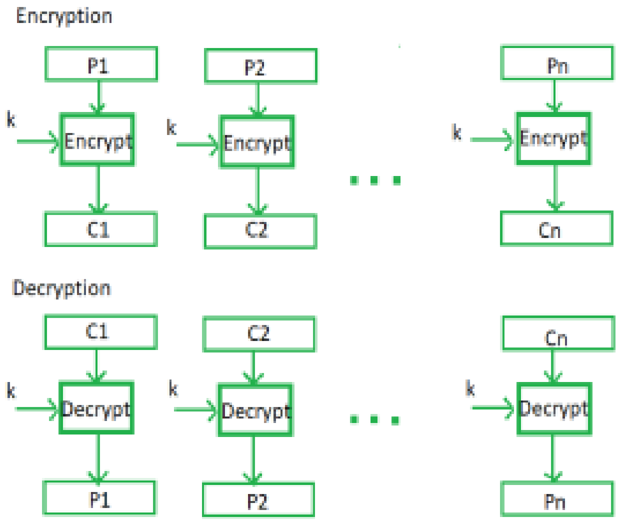
Methods:

Different methods of Block Cipher mode of operations: -

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 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.

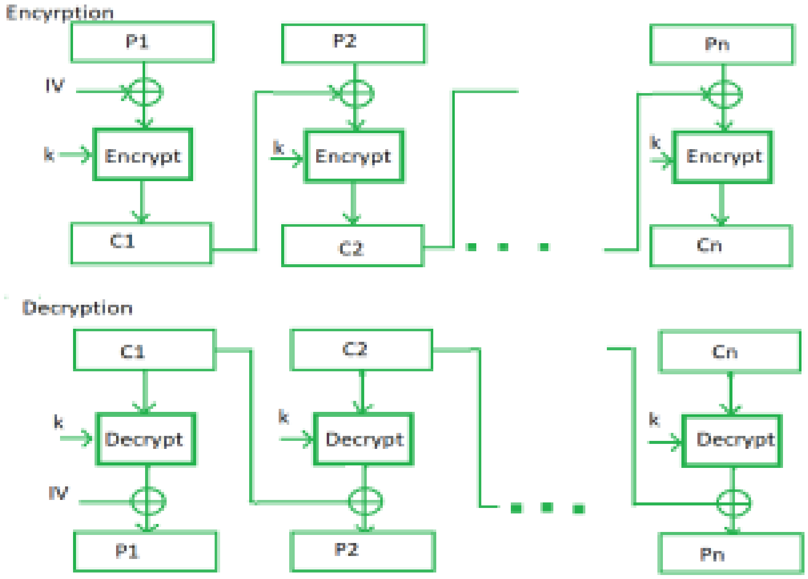
Procedure of ECB is illustrated below:



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 a XOR output of the previous cipher block and the present plaintext block.

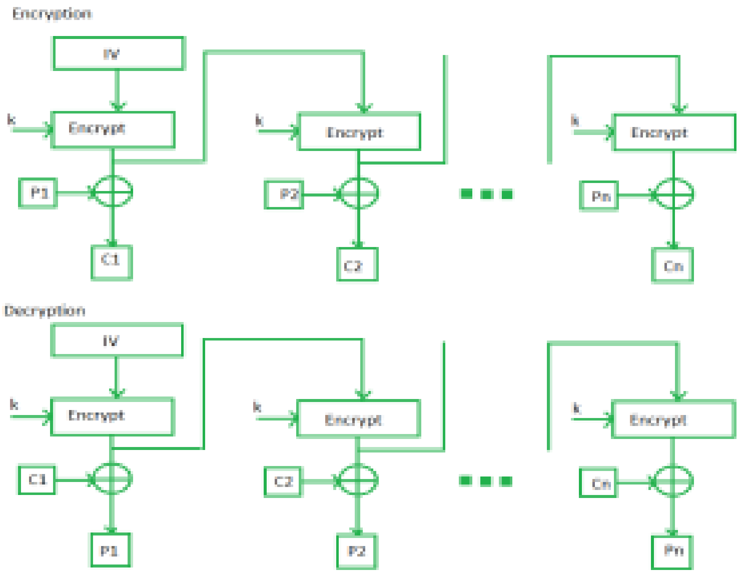
Procedure of CBC is illustrated below:



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 dependency or relationship of cipher on plaintext.

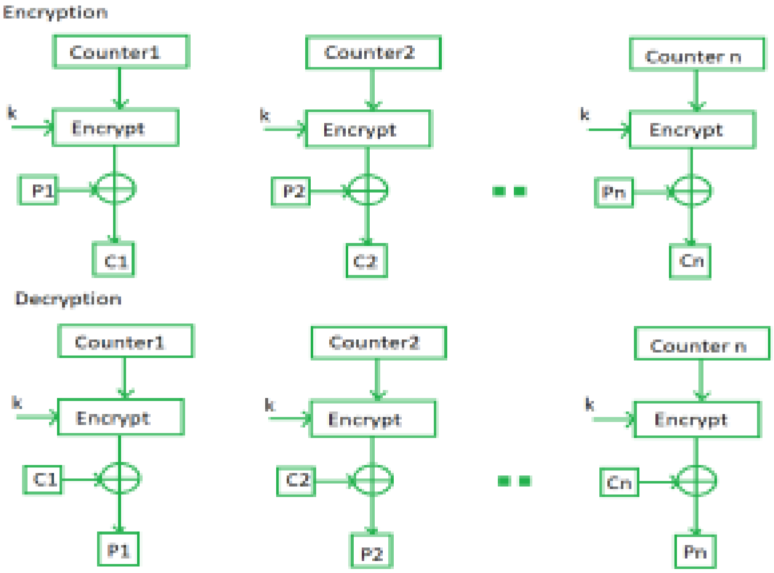
Procedure of Output Feedback Mode is illustrated below:



4. Counter Mode –

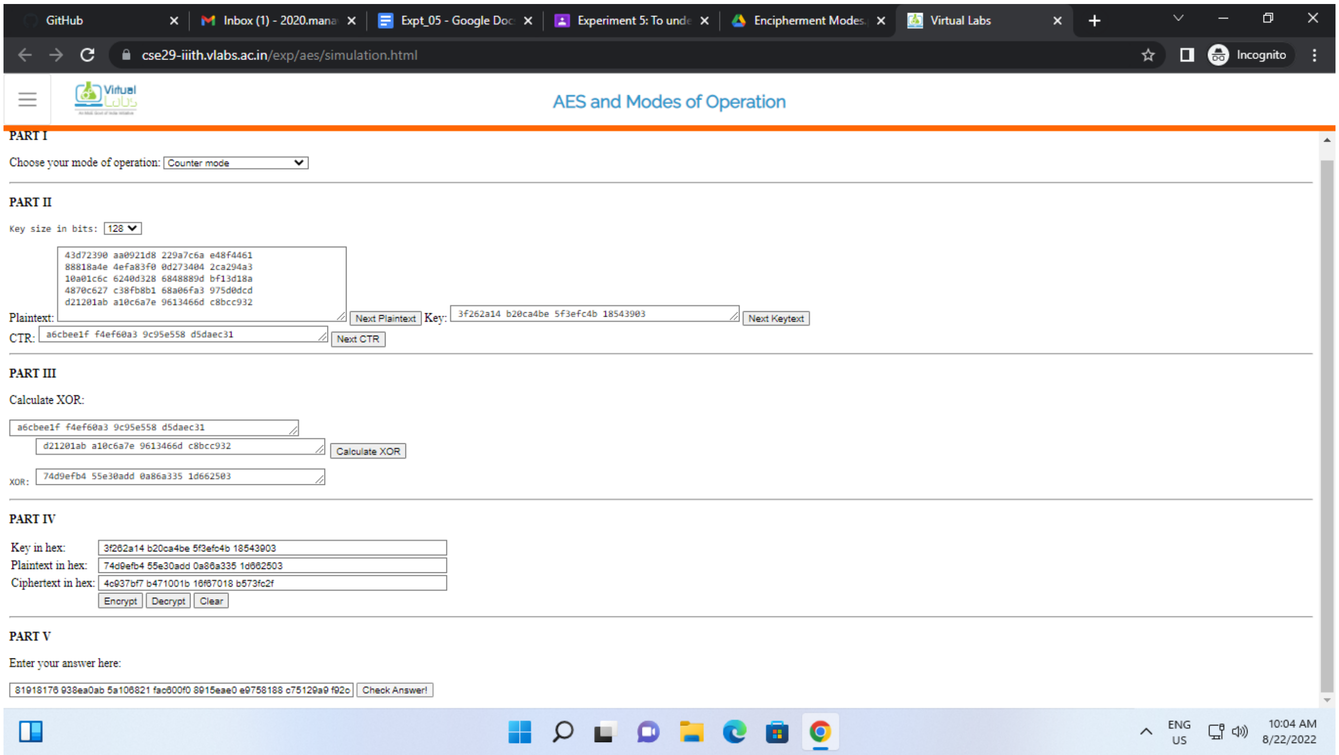
The Counter Mode or CTR is a simple counter-based block cipher implementation. Every time a counter initiated value is encrypted and given as input to XOR with plaintext which results in a ciphertext block. The CTR mode is independent of feedback use and thus can be implemented in parallel.

Procedure of Counter Mode is illustrated below:



Results:

Electronic Code Book:



AES and Modes of Operation

PART I

Choose your mode of operation: Counter mode

PART II

Key size in bits: 128

Plaintext:

```
43d72390 aa0921d8 229a7c6a e48f4461
88818a4e 4efa83f0 0d273404 2ca294a3
10a01c6c 6240d328 6848889d bf13d18a
4870c627 c38fb8b1 68a06fa3 975d0dcd
d21201ab a10c6a7e 9613466d c8bcc932
```

Next Plaintext

Key: 3f262a14 b20ca4be 5f3efc4b 18543903

Next Keytext

CTR: a6cbee1f f4ef60a3 9c95e558 d5daec31

Next CTR

PART III

Calculate XOR:

a6cbee1f f4ef60a3 9c95e558 d5daec31

d21201ab a10c6a7e 9613466d c8bcc932

Calculate XOR

XOR: 74d9efb4 55e30add 0a86a335 1d662503

PART IV

Key in hex: 3f262a14 b20ca4be 5f3efc4b 18543903

Plaintext in hex: 74d9efb4 55e30add 0a86a335 1d662503

Ciphertext in hex: 4c937bf7 b471001b 16f67018 b573fc2f

Encrypt Decrypt Clear

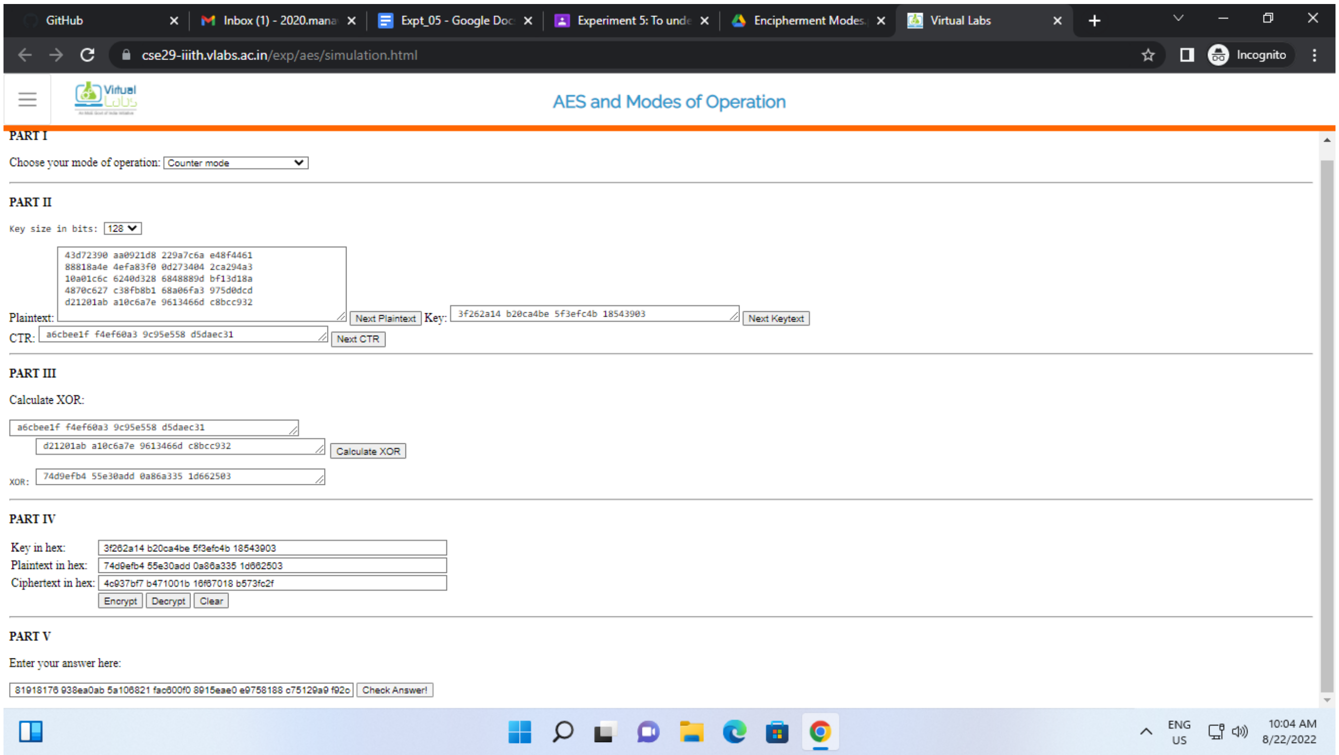
PART V

Enter your answer here:

81918176 938ea0ab 5a106821 fac600f0 8915eae0 e9758188 c75129a9 f92c

Check Answer!

Cipher Block Chaining:



AES and Modes of Operation

PART I

Choose your mode of operation: Counter mode

PART II

Key size in bits: 128

Plaintext:

43d72390 aa0921d8 229a7c6a e48f4461
88818a4e 4efa83f0 0d273404 2ca294a3
10a01c6c 6240d328 6848889d bf13d18a
4870c627 c38fb8b1 68a06fa3 975d0dcd
d21201ab a10c6a7e 9613466d c8bcc932

Next Plaintext

Key: 3f262a14 b20ca4be 5f3efc4b 18543903

Next Keytext

CTR: a6cbee1f f4ef60a3 9c95e558 d5daec31

Next CTR

PART III

Calculate XOR:

a6cbee1f f4ef60a3 9c95e558 d5daec31

d21201ab a10c6a7e 9613466d c8bcc932

Calculate XOR

XOR: 74d9efb4 55e30add 0a86a335 1d662503

PART IV

Key in hex: 3f262a14 b20ca4be 5f3efc4b 18543903

Plaintext in hex: 74d9efb4 55e30add 0a86a335 1d662503

Ciphertext in hex: 4c937bf7 b471001b 16f67018 b573fc2f

Encrypt Decrypt Clear

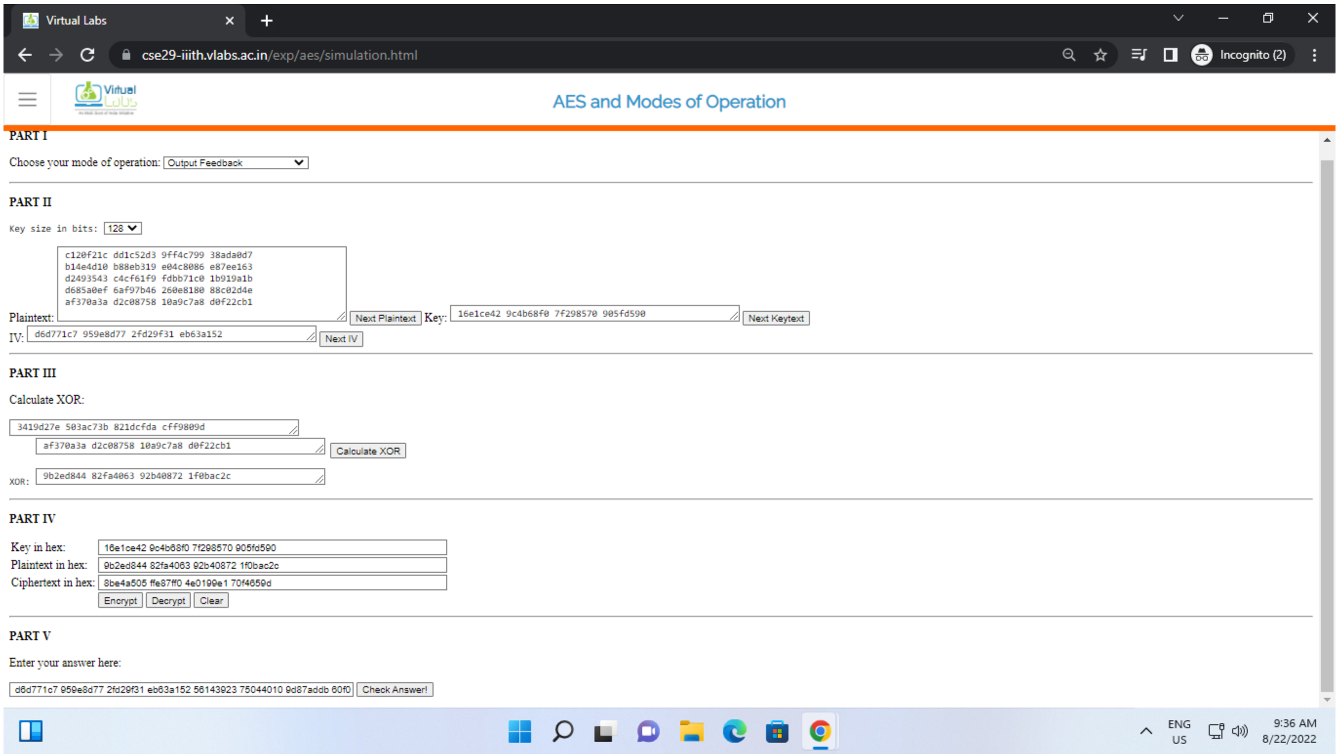
PART V

Enter your answer here:

81918176 938ea0ab 5a106821 fac600f0 8915eae0 e9758188 c75129a9 f92c

Check Answer!

Output Feedback:


Virtual Labs
cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
Incognito (2)
Virtual Labs
AES and Modes of Operation
ENG US
9:36 AM 8/22/2022

PART I

Choose your mode of operation: Output Feedback

PART II

Key size in bits: 128

Plaintext:

```
c120f21c dd1c52d3 9ff4c799 38ada0d7
b14e4d10 b88eb319 e04c8086 e87ee163
d2493543 c4cf61f9 fdbb71c0 1b919a1b
d685a0ef 6af97b46 260e8180 88c02d4e
af370a3a d2c08758 10a9c7a8 d0f22cb1
```

Next Plaintext

Key: 16e1ce42 9c4b68f0 7f298570 905fd590 Next Keytext

IV: d6d771c7 959e8d77 2fd29f31 eb63a152 Next IV

PART III

Calculate XOR:

3419d27e 503ac73b 821dcfda cff9809d

af370a3a d2c08758 10a9c7a8 d0f22cb1 Calculate XOR

XOR: 9b2ed844 82fa4063 92b40872 1f0bac2c

PART IV

Key in hex: 16e1ce42 9c4b68f0 7f298570 905fd590

Plaintext in hex: 9b2ed844 82fa4063 92b40872 1f0bac2c

Ciphertext in hex: 8be4a505 ffe87ff0 4e0199e1 70f4659d

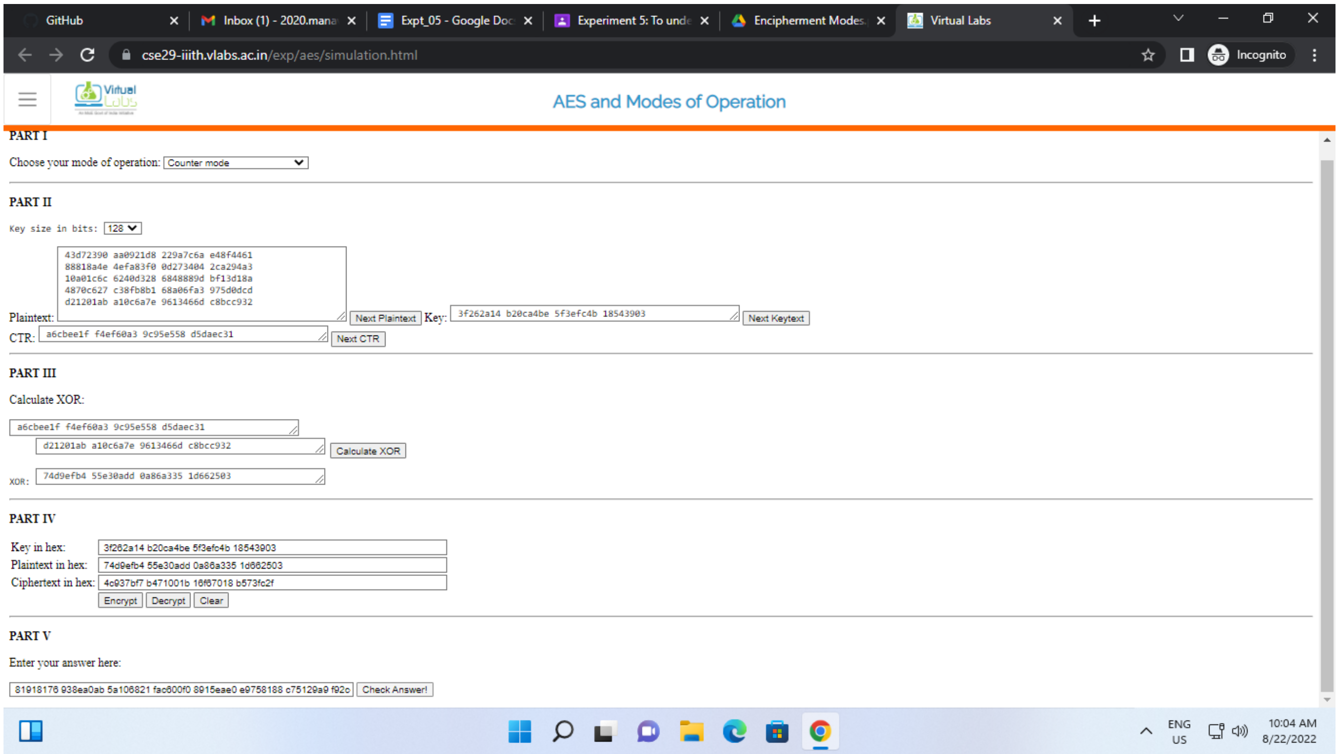
Encrypt Decrypt Clear

PART V

Enter your answer here:

d6d771c7 959e8d77 2fd29f31 eb63a152 56143923 75044010 9d87addb 60f0 Check Answer!

Counter Mode:



PART I

Choose your mode of operation: Counter mode

PART II

Key size in bits: 128

Plaintext:

```
43d72390 aa0921d8 229a7c6a e48f4461
88818a4e 4efa83f0 0d273404 2ca294a3
10a01c6c 6240d328 6848889d bf13d18a
4870c627 c38fb8b1 68a06fa3 975d0dcd
d21201ab a10c6a7e 9613466d c8bcc932
```

Next Plaintext

Key: 3f262a14 b20ca4be 5f3efc4b 18543903 Next Keytext

CTR: a6cbee1f f4ef60a3 9c95e558 d5daec31 Next CTR

PART III

Calculate XOR:

a6cbee1f f4ef60a3 9c95e558 d5daec31

d21201ab a10c6a7e 9613466d c8bcc932 Calculate XOR

XOR: 74d9efb4 55e30add 0a86a335 1d662503

PART IV

Key in hex: 3f262a14 b20ca4be 5f3efc4b 18543903

Plaintext in hex: 74d9efb4 55e30add 0a86a335 1d662503

Ciphertext in hex: 4c937bf7 b471001b 16f67018 b573fc2f

Encrypt Decrypt Clear

PART V

Enter your answer here:

81918176 938ea0ab 5a106821 fac600f0 8915eae0 e9758188 c75129a9 f92c Check Answer!

Conclusion:

We understand how to Encrypt long messages using various modes of operation using the AES.