

Name: Alphonz George

Batch: T11-03

Subject: Security Lab-Assignment 3

Aim: **Block Cipher Modes of operation Theory:**

### **Common Block Cipher Modes of Operation**

#### **1. Electronic Code Book (ECB):**

- Simplest mode: Each plaintext block is encrypted independently.
- Vulnerable to frequency analysis due to identical ciphertext blocks for identical plaintext blocks.
- Rarely used in practice due to security concerns.

#### **2. Cipher Block Chaining (CBC):**

- Each plaintext block is XORed with the previous ciphertext block before encryption.
- Introduces dependency between blocks, improving security.
- Requires an initialization vector (IV) for the first block.

#### **3. Cipher Feedback (CFB):**

- Converts a block cipher into a stream cipher.
- Previous ciphertext is encrypted, and the result is XORed with the plaintext to produce the ciphertext.
- Similar to CBC but with feedback based on ciphertext.

#### **4. Output Feedback (OFB):**

- Another stream cipher mode.
- Generates a keystream by encrypting a counter.
- Keystream is XORed with plaintext to produce ciphertext.

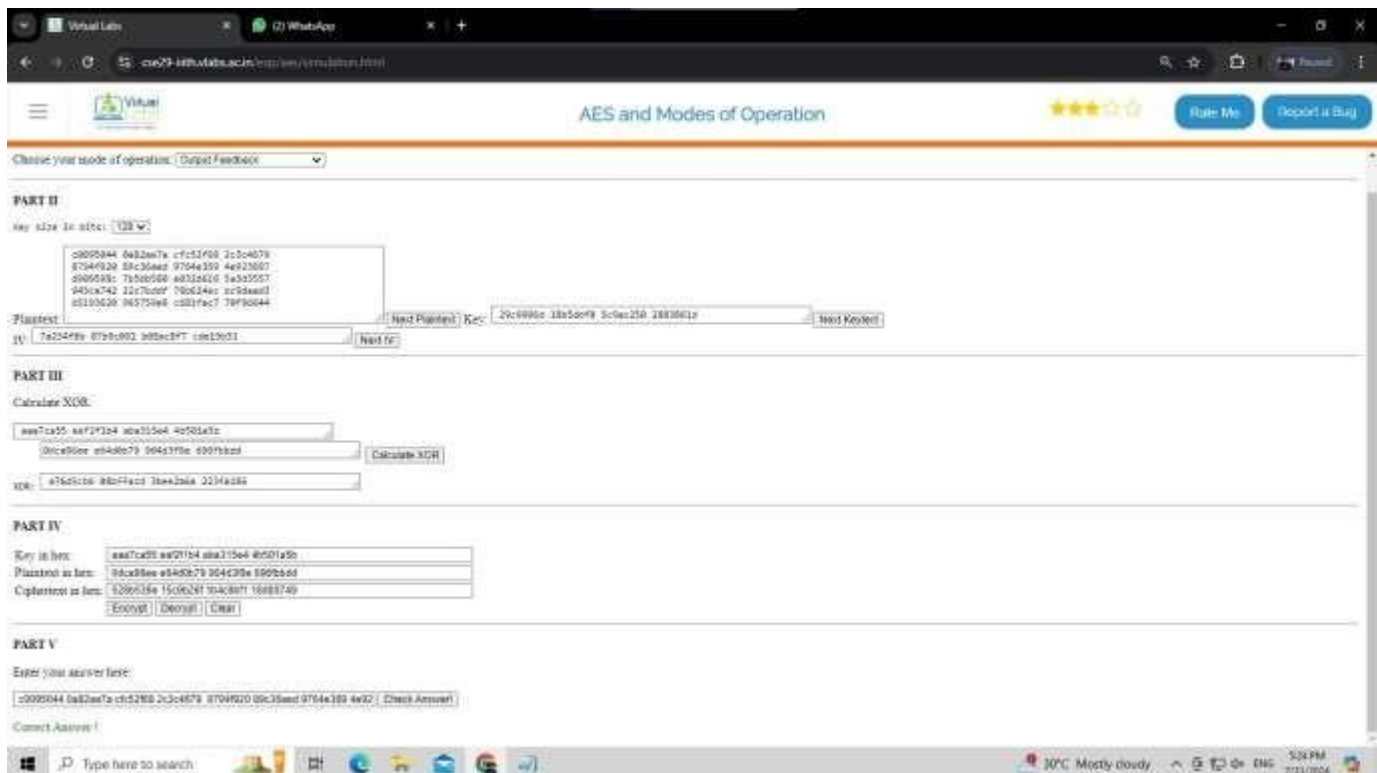
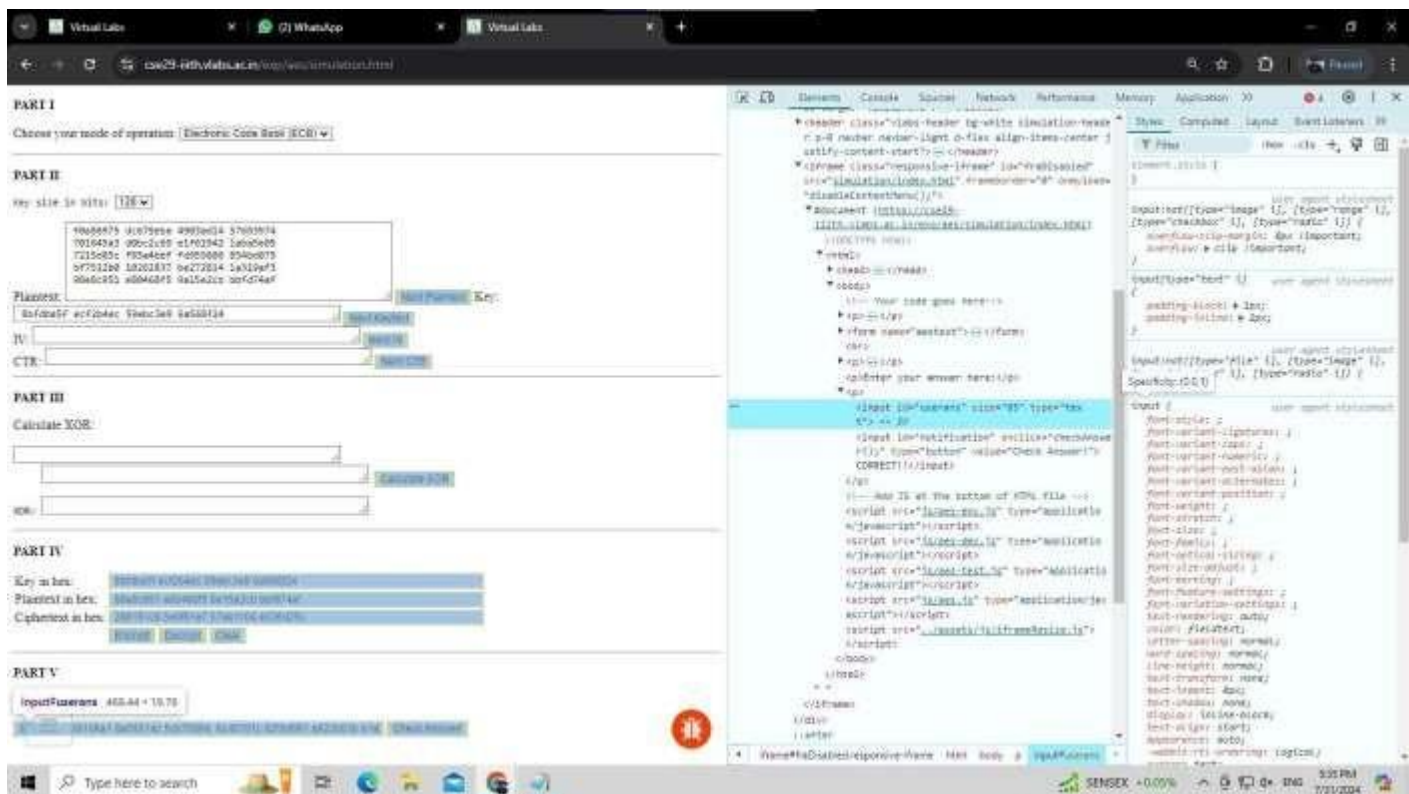
#### **5. Counter (CTR):**

- Similar to OFB but uses a counter instead of feedback.
- Provides high performance and can be parallelized.
- Offers advantages in terms of error propagation and random access.

### **Key Considerations**

- **Security:** Different modes offer varying levels of security against attacks.
- **Performance:** Some modes are more efficient than others.
- **Error propagation:** Some modes are more resilient to bit errors.
- **Random access:** Some modes allow for random access to ciphertext blocks.

### Implementation:



Virtual Lab

(4) WhatsApp

6025-isthvlab-academy/simulation.html

Search

Report

Virtual Lab

AES and Modes of Operation

★★★★☆ Rate Me Report a Bug

Choose your mode of operation: Counter mode

**PART II**  
Key size in bits: 128  

40cc2a0d 384f1c5f 3501c0b8 5f10ba5e  
0c3f100a 8efc0610 2e50ac48 a500603d  
f4a83010 c87f2a00 4c010017 9d200a24  
a0731020 8e23a004 19cc0014 80177501  
cbe8201a 1a8f91a1 3c0a1190 143cd80a

Plaintext: 01900001 22500000 30001100 01911100 Next Plaintext (Key) Next Keyed?  
CTR: 00000000 00000000 00000000 00000000 Next CTR

**PART III**  
Calculate XOR:  

00000000 00000000 00000000 00000000  
01900001 22500000 30001100 01911100

Calculate XOR  
xor: 01900001 22500000 30001100 01911100

**PART IV**  
Key in hex: 00000000 00000000 00000000 00000000  
Plaintext in hex: 01900001 22500000 30001100 01911100  
Ciphertext in hex: 00000000 00000000 00000000 00000000  
Encrypt Decrypt Clear

**PART V**  
Enter your answer here:  
01900001 22500000 30001100 01911100 Check Answer!  
Current Answer: /

Type here to search

Taskbar icons: File Explorer, Edge, WhatsApp, etc.

System tray: Near record, 3:27 PM, 7/31/2024

Virtual Labs

CI WhatsApp

coe79-lab4lab.ac.in/en/virtual-lab.html

Virtual Labs

AES and Modes of Operation

★★★★☆

Run Me

Report a Bug

Choose your mode of operation: Single Block Chaining

**PART II**

Key size in bits: 128

8a67ca00 9f371b4 0a033a4 40501a0  
70e4b3c 0320a14 13453a0 8079c3a  
05c1c55 78f9ac0 1252a7d 8c81c1f  
2750a7f 8a60c0c 40f2c00 420a1a0  
0a24300 c2a7012 01000a1 7045f90

Next Plaintext

Key: 0ca08a 04a070 04a070 04a070

Next Keybit

IV:

Next IV

**PART III**

Calculate XOR:

0e24290 82a7c00 01c095a1 79a0f88

01ce00e 04a070 04a070 00f1a0

Calculate XOR

XOR: 01a0200 30a000 2f1a01f 02a0400

**PART IV**

Key in hex: 0ca08a 04a070 04a070 04a070

Plaintext in hex: 0e24290 82a7c00 01c095a1 79a0f88

Ciphertext in hex: 79a0f88 42a0500 01a0200 02a0400

Encrypt Decrypt Clear

**PART V**

Enter your answer here:

24a0001 0020c30 4320c47 0500040 5e5006a 747033d checkall six Check Answer

Correct Answer!

Type here to search

SAP 500 +1.18%

5:15 PM 7/11/2024

Virtual Labs

o25-10hvlabs.academy/simulation.html

AES and Modes of Operation

★★★★☆

Rate Me

Report a Bug

PART II

Key size in bits: 128

8007c03b 4e49f1b4 89a113ec 8c0f1a8b  
73c9433c 2123a14 139a3a08 05795428  
85c1c353 78f9ac09 125267e8 8c01c3f  
c759e7ff 2e90000c 40f95188 412a1a82  
8e242558 02a70010 31000541 7945f988

Next Plaintext

Next Key

Plaintext: 

8e242558 02a70010 31000541 7945f988

Next Plaintext

IV: 

8007c03b 4e49f1b4 89a113ec 8c0f1a8b

Next IV

CTR: 

8007c03b 4e49f1b4 89a113ec 8c0f1a8b

Next CTR

PART III

Calculate XOR:

8e242558 02a70010 31000541 7945f988

8007c03b 4e49f1b4 89a113ec 8c0f1a8b

Calculate XOR

XOR: 

0029800a e449070 93a0550a 999e001

PART IV

Key in hex: 0029800a e449070 93a0550a 999e001

Plaintext in hex: 00000000 34400004 2155a03f 10244245

Ciphertext in hex: 706078a 42e05d05 07e020e 1371a263

Encrypt Decrypt Clear

PART V

Enter your answer here:

24a18031 8820c378 4329c47 00000045 5a00000a 747833a5 0b000000 00000000

Check Answer!

Current Answer: /

Type here to search

30°C Mostly cloudy

2:08 PM 11/31/2024