Name: Alphonz George

Batch: T11-03

Subject: Security Lab-Assignment 3

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

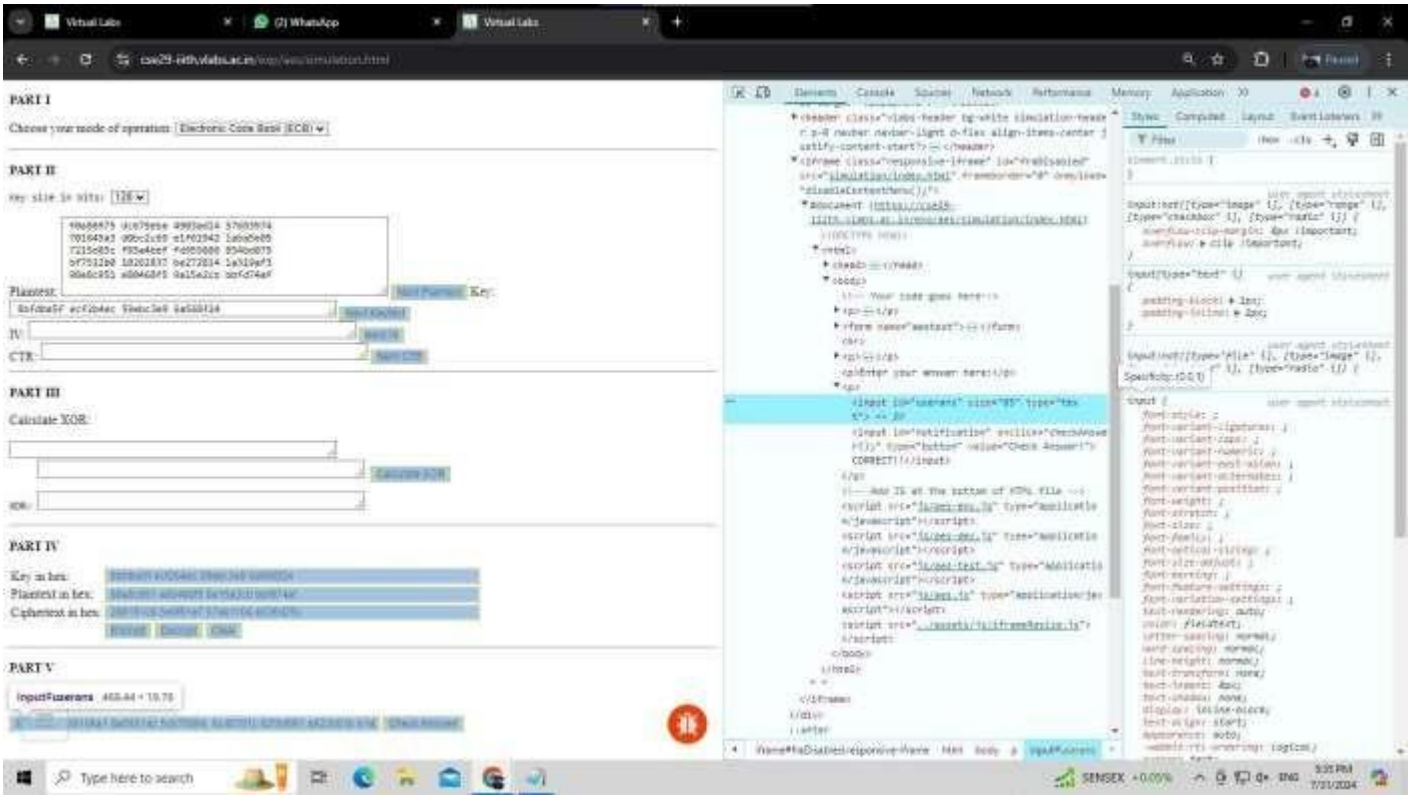
Common Block Cipher Modes of Operation

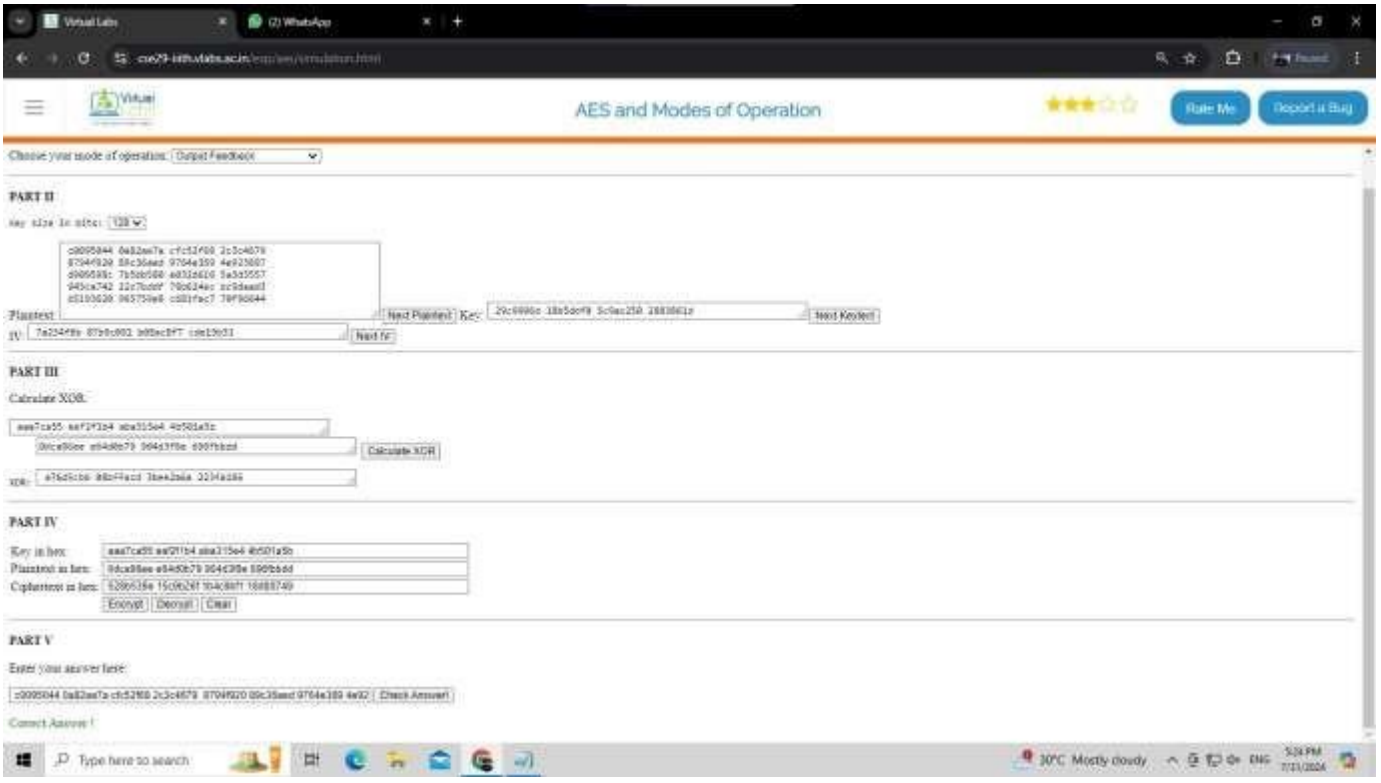
1. **Electronic Code Book (ECB):**
    - Simplest mode: Each plaintext block is encrypted independently.
    - Vulnerable to frequency analysis due to identical ciphertext blocks for identical plaintext blocks.
    - Rarely used in practice due to security concerns.
2. **Cipher Block Chaining (CBC):**
    - 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.

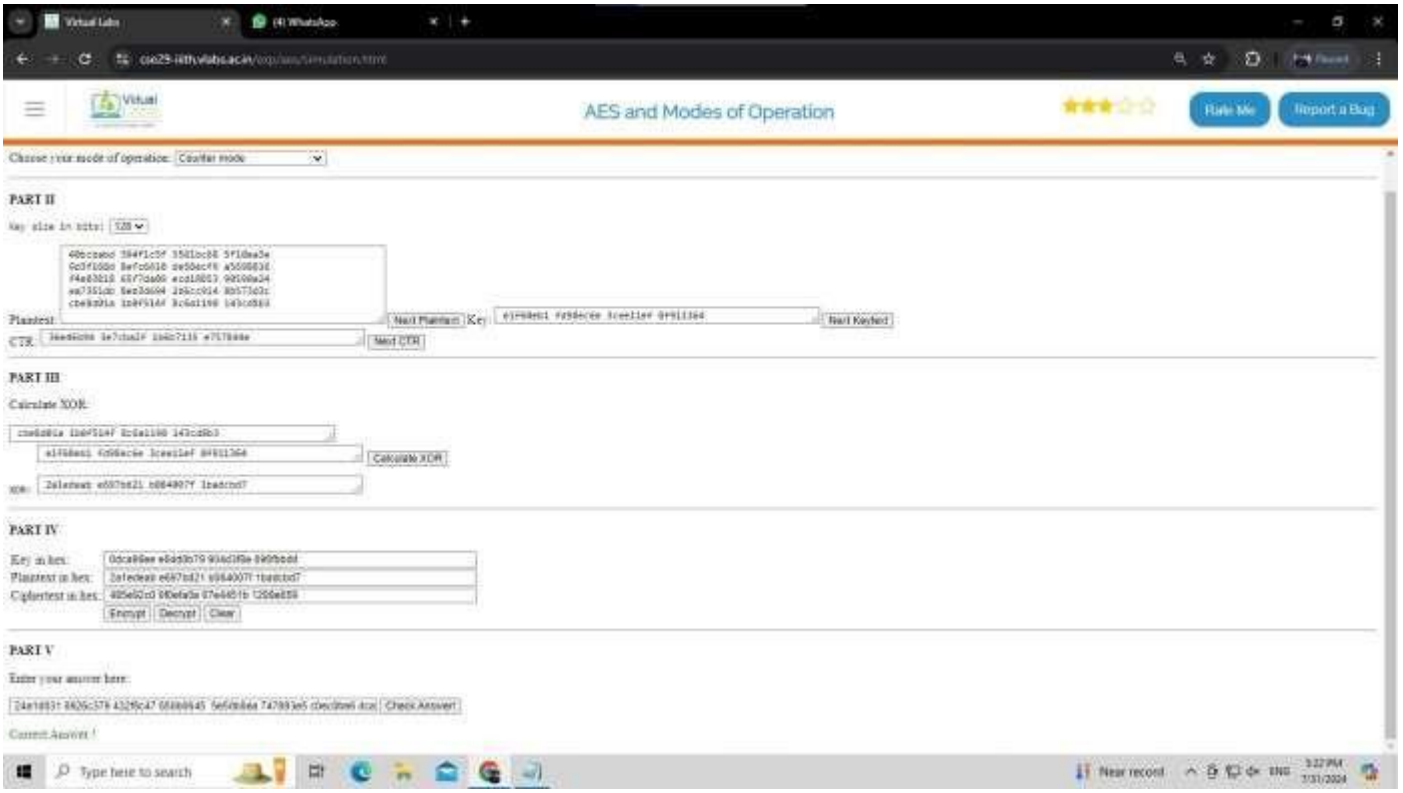
Key Considerations

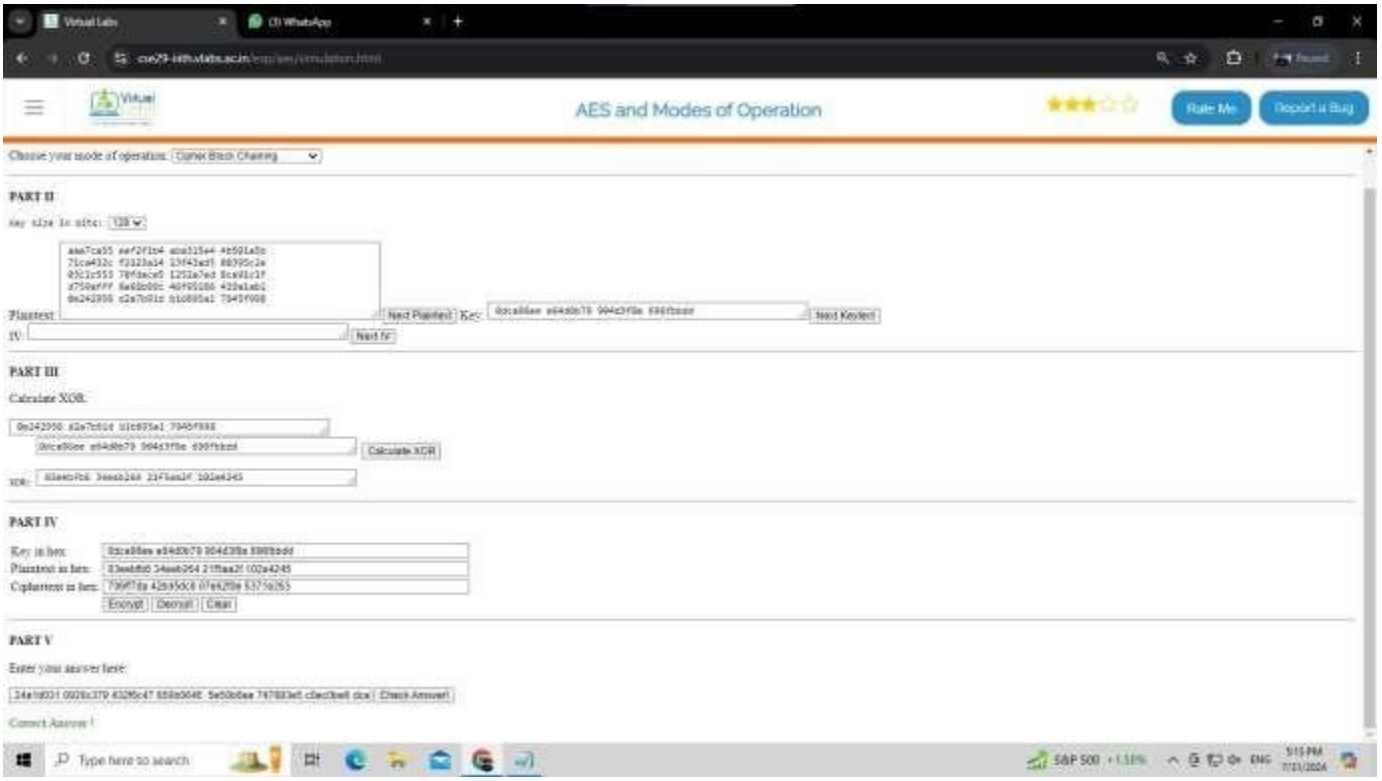
- **Security:** Different modes offer varying levels of security against attacks.
- **Performance:** Some modes are more efficient than others.
- **Error propagation:** Some modes are more resilient to bit errors.
- **Random access:** Some modes allow for random access to ciphertext blocks.

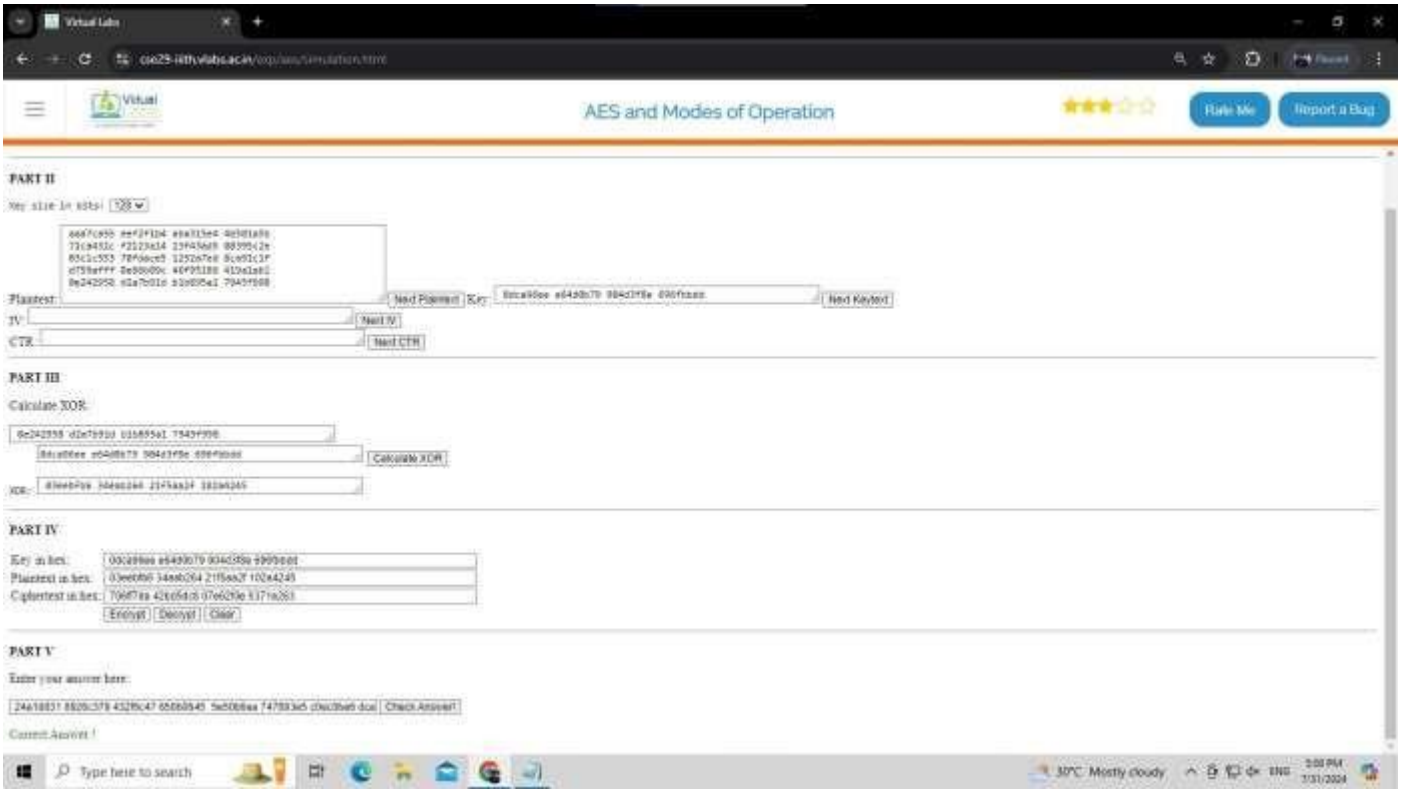
Implementation:






AES and Modes of Operation
Rate Me
Report a Bug
Choose your mode of operation:
Counter mode
PART II
Key size in bits:
128
Plaintext:
Next Plaintext
Key:
Next Keytext
CTR:
Next CTR
PART III
Calculate XOR:
Calculate XOR
XOR:
PART IV
Key in hex:
Plaintext in hex:
Ciphertext in hex:
Encrypt
Decrypt
Clear
PART V
Enter your answer here:
Check Answer
Correct Answer !
Type here to search


Virtual Labs
(3) WhatsApp
AES and Modes of Operation
Rate Me
Report a Bug
Choose your mode of operation:
Cipher Block Chaining
PART II
Key size in bits:
128
Plaintext:
Next Plaintext
Key:
Next Keytext
IV:
Next IV
PART III
Calculate XOR:
Calculate XOR
XOR:
PART IV
Key in hex:
Plaintext in hex:
Ciphertext in hex:
Encrypt
Decrypt
Clear
PART V
Enter your answer here:
Check Answer!
Correct Answer !
Type here to search
S&P 500 +1.16%
ENG
5:15 PM
7/21/2024


Virtual Labs
AES and Modes of Operation
Rate Me
Report a Bug
PART II
Key size in bits:
Plaintext:
Next Plaintext
Key:
Next Keytext
IV:
Next IV
CTR:
Next CTR
PART III
Calculate XOR:
Calculate XOR
XOR:
PART IV
Key in hex:
Plaintext in hex:
Ciphertext in hex:
Encrypt
Decrypt
Clear
PART V
Enter your answer here:
Check Answer!
Correct Answer !
Type here to search
30°C Mostly cloudy
ENG