Subject: Security Lab-Assignment 3

Aim: **Block Cipher Modes of operation**

Theory:

Common Block Cipher Modes of Operation

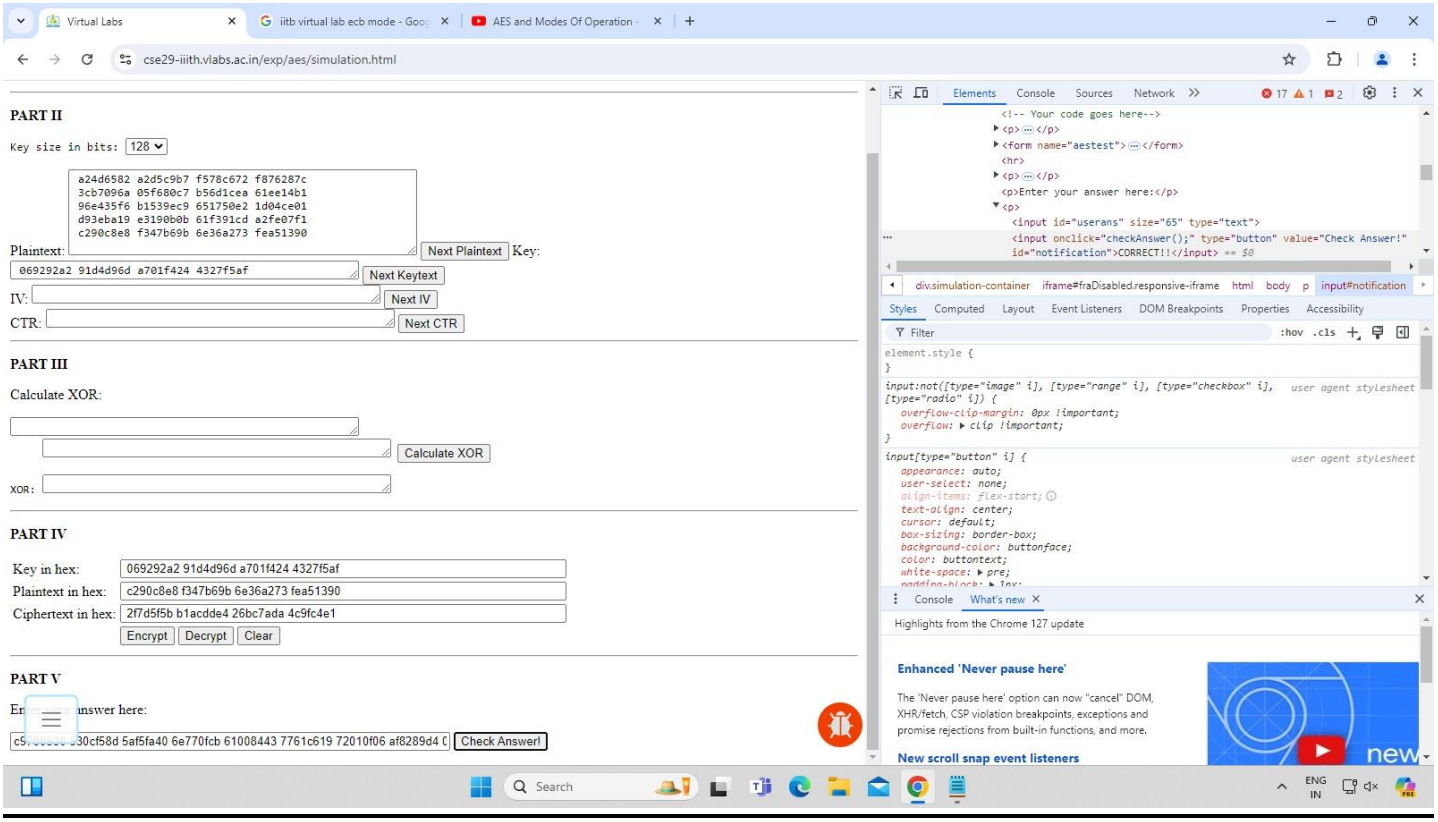
1. **Electronic Code Book (ECB):**
    - Simplest mode: Each plaintext block is encrypted independently. ○ Vulnerable to frequency analysis due to identical ciphertext blocks for identical plaintext blocks.
    - Rarely used in practice due to security concerns.
2. **Cipher Block Chaining (CBC):**
 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

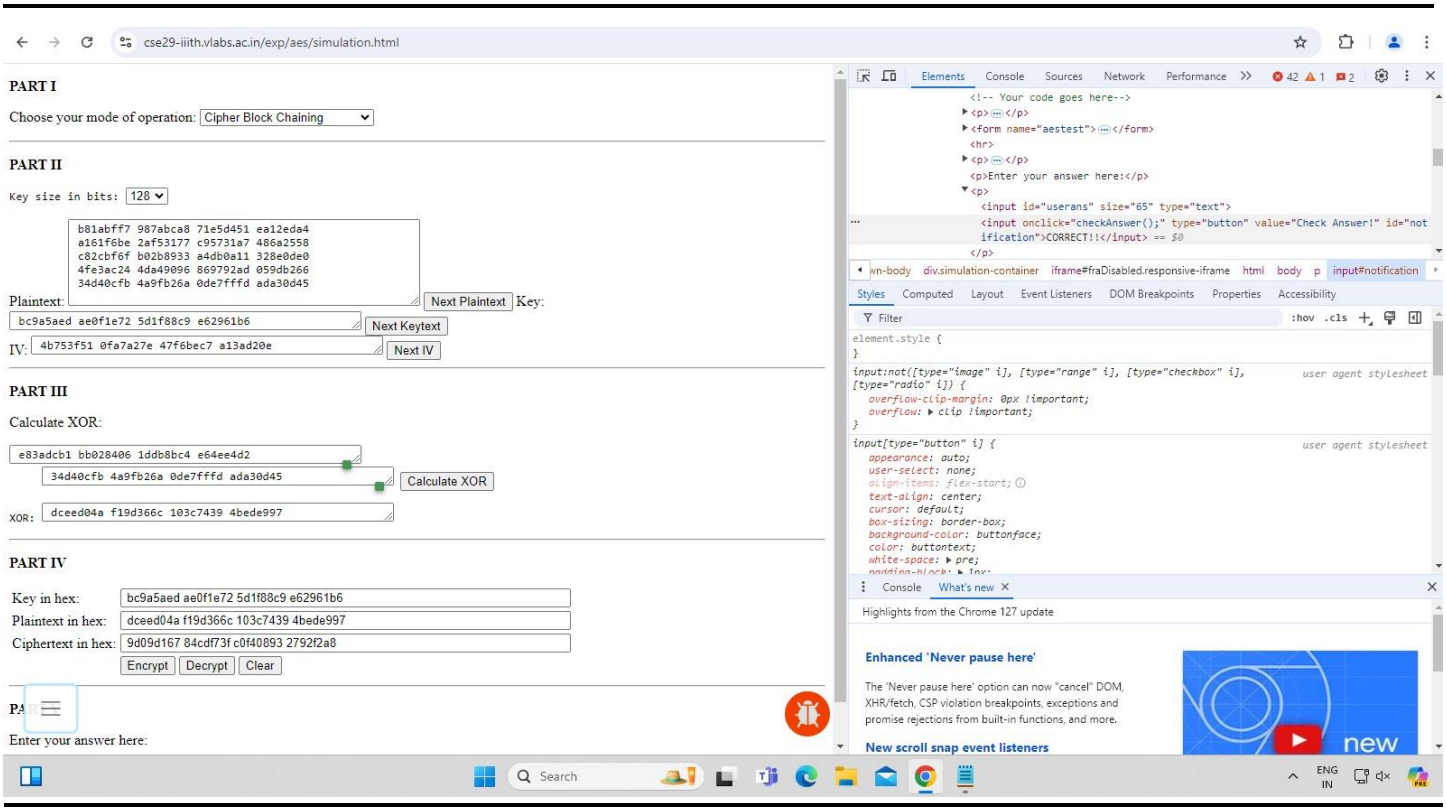
Key Considerations

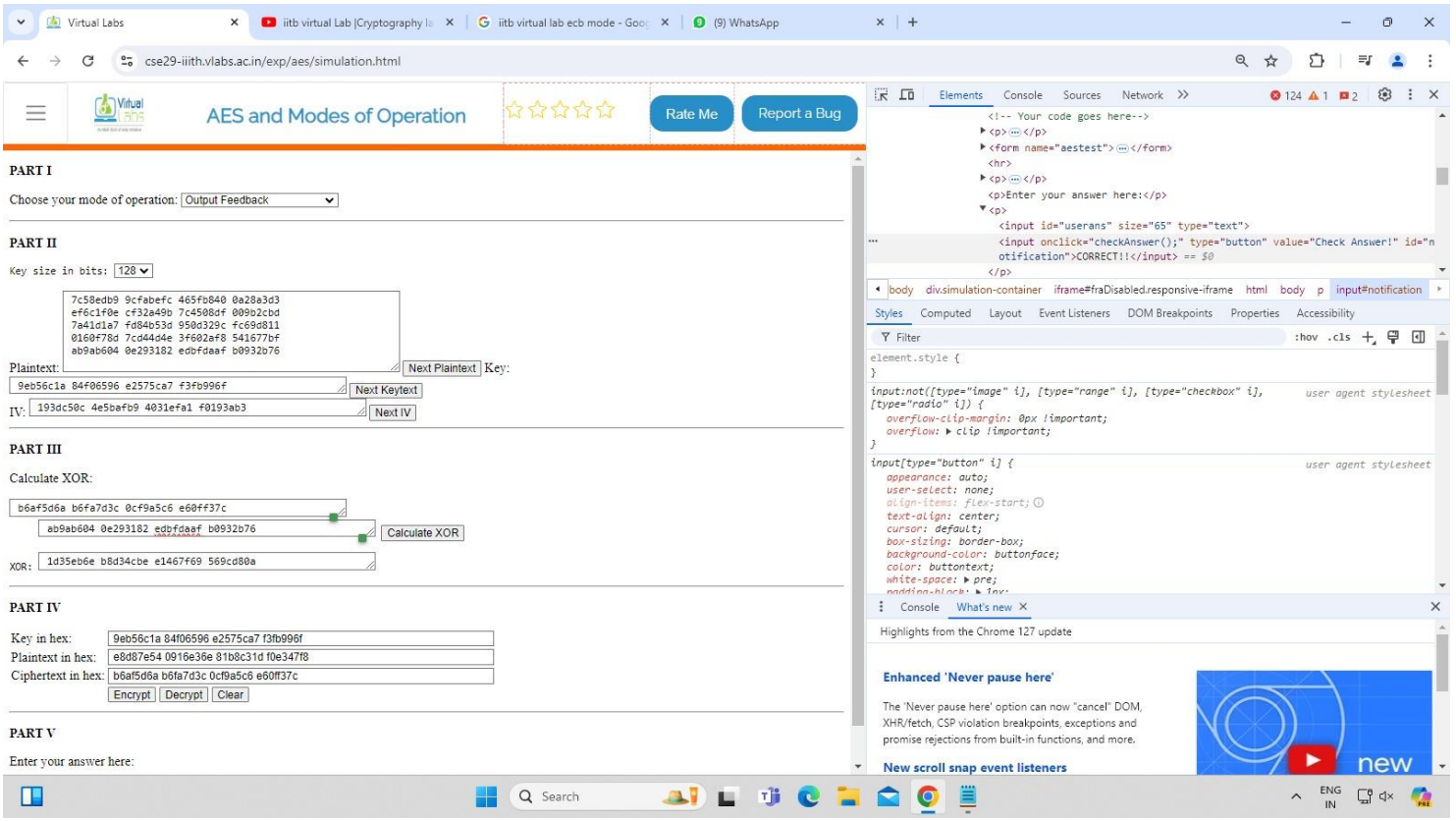
- **Security:** Different modes offer varying levels of security against attacks.

- **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 Labs
iitb virtual Lab |Cryptography la
iitb virtual lab ecb mode - Goo
(9) WhatsApp
cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
AES and Modes of Operation
Rate Me
Report a Bug
PART I
Choose your mode of operation: Output Feedback
PART II
Key size in bits: 128
7c58edb9 9cfabefc 465fb840 0a28a3d3
ef6c1f0e cf32a49b 7c4508df 009b2cbd
7a41d1a7 fd84b53d 950d329c fc69d811
0160f78d 7cd44d4e 3f602af8 541677bf
ab9ab604 0e293182 edbfdaaf b0932b76
Plaintext:
Next Plaintext
Key:
9eb56c1a 84f06596 e2575ca7 f3fb996f
Next Keytext
IV:
193dc50c 4e5bafb9 4031efa1 f0193ab3
Next IV
PART III
Calculate XOR:
b6af5d6a b6fa7d3c 0cf9a5c6 e60ff37c
ab9ab604 0e293182 edbfdaaf b0932b76
Calculate XOR
XOR:
1d35eb6e b8d34cbe e1467f69 569cd80a
PART IV
Key in hex:
9eb56c1a 84f06596 e2575ca7 f3fb996f
Plaintext in hex:
e8d87e54 0916e36e 81b8c31d f0e347f8
Ciphertext in hex:
b6af5d6a b6fa7d3c 0cf9a5c6 e60ff37c
Encrypt
Decrypt
Clear
PART V
Enter your answer here:
Elements
Console
Sources
Network
<!-- Your code goes here-->

<form name="aestest"></form>
<hr>

Enter your answer here:

<input id="userans" size="65" type="text">
<input onclick="checkAnswer();" type="button" value="Check Answer!" id="notification">CORRECT!!</input> == $0

body
div.simulation-container
iframe#fraDisabled.responsive-iframe
html
body
p
input#notification
Styles
Computed
Layout
Event Listeners
DOM Breakpoints
Properties
Accessibility
Filter
:hov .cls
element.style {
}
input:not([type="image" i], [type="range" i], [type="checkbox" i], [type="radio" i]) {
overflow-clip-margin: 0px !important;
overflow: clip !important;
}
user agent stylesheet
input[type="button" i] {
appearance: auto;
user-select: none;
align-items: flex-start;
text-align: center;
cursor: default;
box-sizing: border-box;
background-color: buttonface;
color: buttontext;
white-space: pre;
}
user agent stylesheet
Console
What's new
Highlights from the Chrome 127 update
Enhanced 'Never pause here'
The 'Never pause here' option can now "cancel" DOM, XHR/fetch, CSP violation breakpoints, exceptions and promise rejections from built-in functions, and more.
New scroll snap event listeners
new
Search
ENG
IN