Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.

LAB ASSIGNMENT NO. 3

AIM: To study Block cipher modes of operation using Advanced Encryption Standard (AES).

LAB OUTCOME ATTAINED:

LO 2: Demonstrate Key management, distribution and user authentication.

THEORY:

AES (Advanced Encryption Standard) is a symmetric-key encryption algorithm, meaning the same key is used for both encryption and decryption. It's a widely adopted encryption standard for securing sensitive data and is known for its efficiency and security.

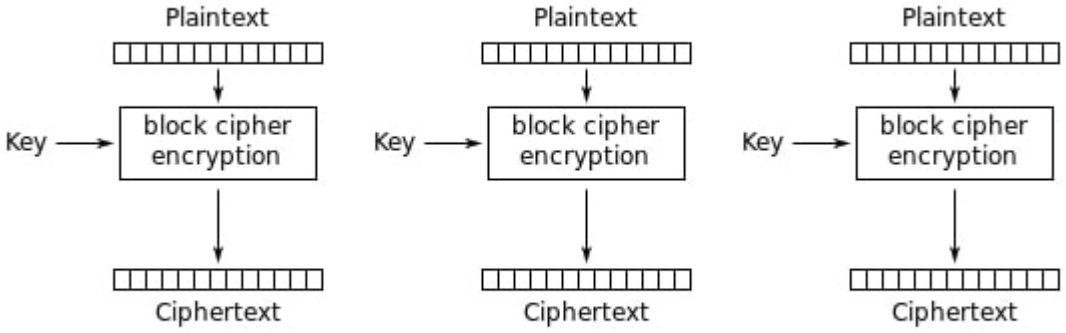
1. **Type of Cipher**: AES is a block cipher, which means it encrypts data in fixed-size blocks (128 bits or 16 bytes) rather than one bit at a time.
2. **Number of Rounds**: The number of rounds in AES depends on the key size. For AES-128, there are 10 rounds; for AES-192, there are 12 rounds; and for AES-256, there are 14 rounds. Each round involves a series of operations.
3. **Key Size**: AES supports key sizes of 128, 192, or 256 bits. The key size determines the security level, with longer keys providing stronger encryption.
4. **Block Size:** AES operates on data blocks of 128 bits (16 bytes). This block size remains fixed regardless of the key size.
5. **Operations in Each Round**: In each round of AES, several operations are performed on the data, including:
    - SubBytes: Non-linear substitution where each byte in the block is replaced with a corresponding byte from a fixed table (called the S-box).
    - ShiftRows: Bytes in each row of the block are shifted left by different offsets.
    - MixColumns: A mathematical mixing operation is performed on the columns of the block.
    - AddRoundKey: The block is XORed with a portion of the expanded encryption key derived from the original encryption key.

Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.

MODES OF OPERATION:

ECB Mode (Electronic Codebook Mode):

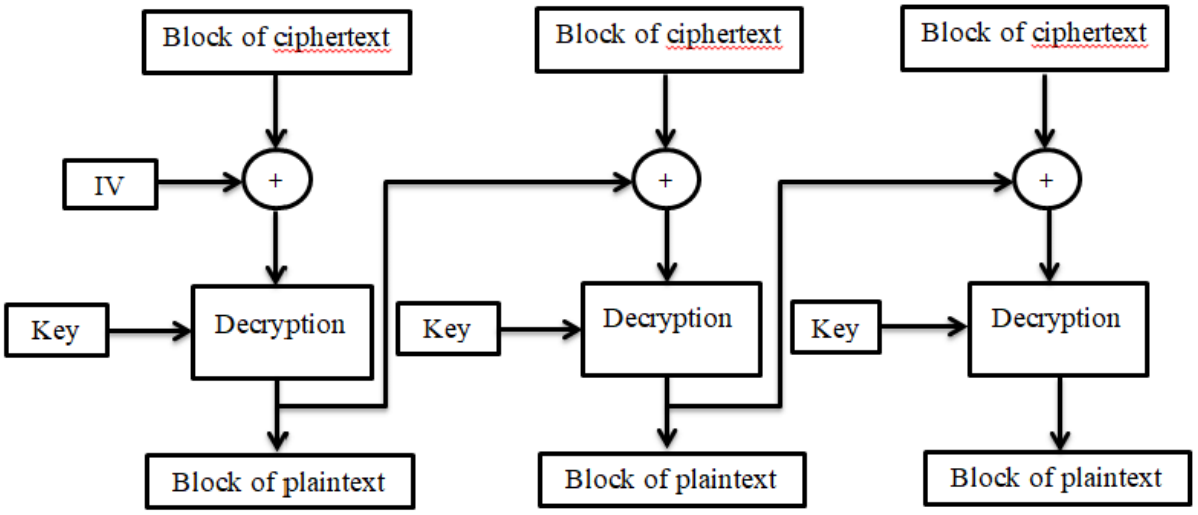
In ECB mode, each block of plaintext is encrypted independently with the same encryption key. This means that identical blocks of plaintext will result in identical blocks of ciphertext, which can be a security vulnerability.



Electronic Codebook (ECB) mode encryption

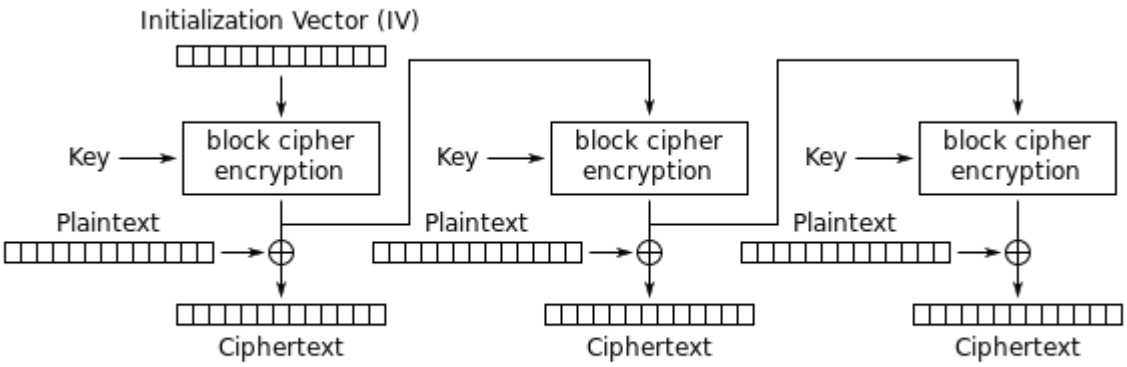
CBC Mode (Cipher Block Chaining Mode):

In CBC mode, each block of plaintext is XORed with the previous ciphertext block before encryption. This "chaining" of blocks adds complexity and ensures that identical plaintext blocks do not produce identical ciphertext blocks.



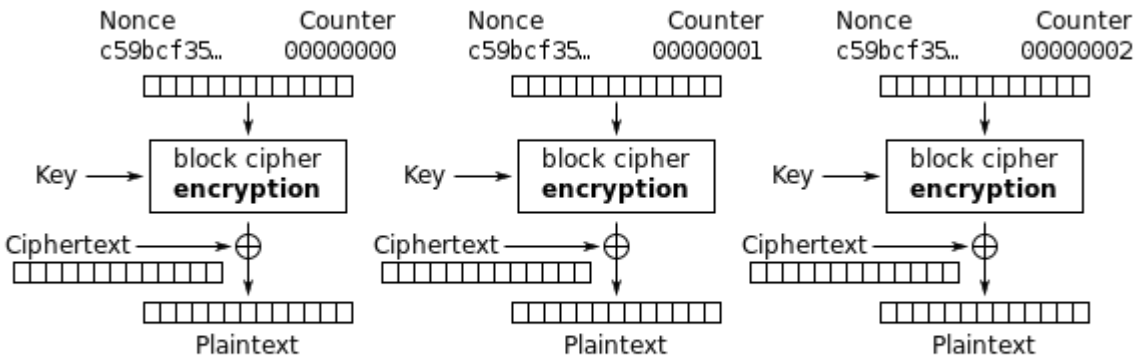
Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.

OFB Mode (Output Feedback Mode):
OFB mode converts the block cipher into a stream cipher. It generates a stream of pseudo-random bits using an initialization vector (IV) and the encryption key. This stream is then XORed with the plaintext to produce ciphertext.



Output Feedback (OFB) mode encryption

Counter Mode (CTR Mode):
Counter mode also converts the block cipher into a stream cipher. It uses a counter value as an IV, which is incremented for each block. The counter value is encrypted to produce a keystream, which is then XORed with the plaintext.



Counter (CTR) mode decryption

Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.

OUTPUT:

PART I

Choose your mode of operation: Electronic Code Book (ECB)

PART II

Key size in bits: 128

Plaintext:
```
38446fd9 643b8207 90f83cd8 927f25ef
1e01bc42 356c2ffa d87caf05 5ebebdf9
2bd7d18e 54e31db7 847c41c3 a78c27db
eb48922a cb1bef7d 261c959e ae006c05
a7280a41 9a6405ee b439bf3d 64a038aa
```
Next Plaintext

Key:
```
1a5951c8 8cbecfff 6ba85166 51b914eb
```
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

Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.

AES and Modes of Operation

Key size in bits: 128

Plaintext:
```
38446fd9 643b8207 90f83cd8 927f25ef
1e01bc42 356c2ffa d87caf05 5ebebdf9
2bd7d18e 54e31db7 847c41c3 a78c27db
eb48922a cb1bef7d 261c959e ae006c05
a7280a41 9a6405ee b439bf3d 64a038aa
```
Next Plaintext Key: 1a5951c8 8cbecfff 6ba85166 51b914eb Next Keytext

IV: Next IV

CTR: Next CTR

PART III

Calculate XOR:

Calculate XOR

XOR:

PART IV

Key in hex: 1a5951c8 8cbecfff 6ba85166 51b914eb

Plaintext in hex: 38446fd9 643b8207 90f83cd8 927f25ef

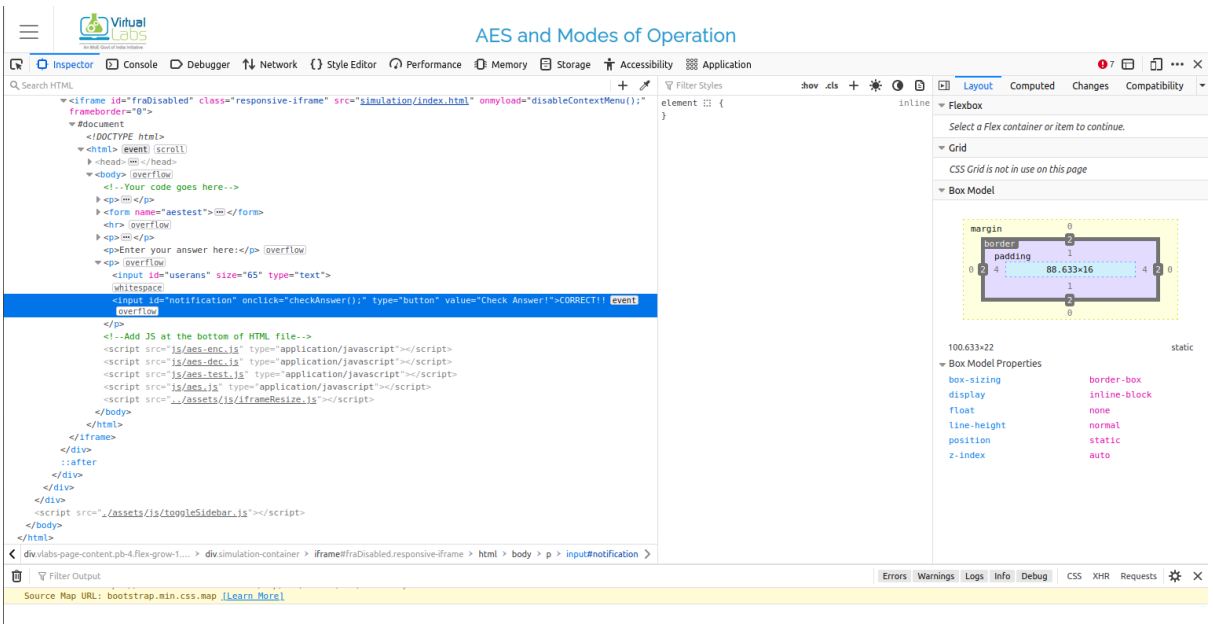
Ciphertext in hex: f7a052ca 81711404 1e47f52a 7761f7ea

Encrypt Decrypt Clear

PART V

Enter your answer here:

f7a052ca 81711404 1e47f52a 7761f7ea Check Answer!



Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.

Inspector | Console | Debugger | Network | Style Editor | Performance | Memory | Storage | Accessibility

Search HTML

```
<div class="vlabs-page-content pb-4 flex-grow-1 markdown-body">
  ::before
  <div class="text-center px-5 fix-spacing">…</div>
  <div class="simulation-container"> flex
    <button id="toggle-menu-float-button" class="btn btn-primary" type="button" data-bs-toggle="modal" data-bs-target="#popupMenu">…</button>
    <header class="vlabs-header bg-white simulation-header p-0 navbar navbar-light d-flex align-items-center justify-content-start">…</header> flex
    <iframe id="fraDisabled" class="responsive-iframe" src="simulation/index.html" onmyload="disableContextMenu();" frameborder="0">
      #document
        <!DOCTYPE html>
        <html> event scroll
          <head>…</head>
          <body> overflow
            <!--Your code goes here-->
            <p>…</p>
            <form name="aestest">…</form>
            <hr> overflow
            <p>…</p>
            <p>Enter your answer here:</p> overflow
            <p> overflow
              <input id="userans" size="65" type="text">
              whitespace
              <input onclick="checkAnswer();" type="button" value="Check Answer!"> event overflow
              <p id="notification">Sorry, answer is wrong. Please try again.</p> overflow
            </p>
            <!--Add JS at the bottom of HTML file-->
            <script src="js/aes-enc.js" type="application/javascript"></script>
            <script src="js/aes-dec.js" type="application/javascript"></script>
            <script src="js/aes-test.js" type="application/javascript"></script>
            <script src="js/aes.js" type="application/javascript"></script>
            <script src="../assets/js/iframeResize.js"></script>
          </body>
        </html>
    </iframe>
  </div>
  ::after
</div>
```

bs-page.d-fl… > div.container-fluid.flex-fill.d-flex.fle… > div.row.flex-grow-1.d-flex.flex-nowrap.f… > div.vlabs-page-content.pb-4.flex-grow-1.… > ::after

Filter Output

Source Map URL: bootstrap.min.css.map [Learn More]

Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.

AES and Modes of Operation

PART I

Choose your mode of operation: Cipher Block Chaining

PART II

Key size in bits: 128

Plaintext:
```
9335300b e2435f9b 7286bd7c 7701d9be
15c7c6c4 c3c32ab2 98d17dfb a1d2b395
584a0e79 083b535a 5b37585a 80576f4e
7863efc4 ed353c4b 2de3520b eb7f4ec1
1414bbfe 19c8c67f 573a51c7 5e9257bb
```
Next Plaintext Key: a90a0373 4ecfdcc5 37f24b3f b6abe197 Next Keytext

IV: 963c73b8 ded48600 49cb817d a3939614 Next IV

PART III

Calculate XOR:

1414bbfe 19c8c67f 573a51c7 5e9257bb

963c73b8 ded48600 49cb817d a3939614 Calculate XOR

XOR: 8228c846 c71c407f 1ef1d0ba fd01c1af

PART IV

Key in hex: a90a0373 4ecfdcc5 37f24b3f b6abe197

Plaintext in hex: 8228c846 c71c407f 1ef1d0ba fd01c1af

Ciphertext in hex: c1b2a50f cba4a942 2d1c8dd5 0a19d0cf

Encrypt Decrypt Clear

AES and Modes of Operation

Key size in bits: 128

Plaintext:
```
9335300b e2435f9b 7286bd7c 7701d9be
15c7c6c4 c3c32ab2 98d17dfb a1d2b395
584a0e79 083b535a 5b37585a 80576f4e
7863efc4 ed353c4b 2de3520b eb7f4ec1
1414bbfe 19c8c67f 573a51c7 5e9257bb
```
Next Plaintext Key: a90a0373 4ecfdcc5 37f24b3f b6abe197 Next Keytext

IV: 963c73b8 ded48600 49cb817d a3939614 Next IV

PART III

Calculate XOR:

1414bbfe 19c8c67f 573a51c7 5e9257bb

963c73b8 ded48600 49cb817d a3939614 Calculate XOR

XOR: 8228c846 c71c407f 1ef1d0ba fd01c1af

PART IV

Key in hex: a90a0373 4ecfdcc5 37f24b3f b6abe197

Plaintext in hex: 8228c846 c71c407f 1ef1d0ba fd01c1af

Ciphertext in hex: c1b2a50f cba4a942 2d1c8dd5 0a19d0cf

Encrypt Decrypt Clear

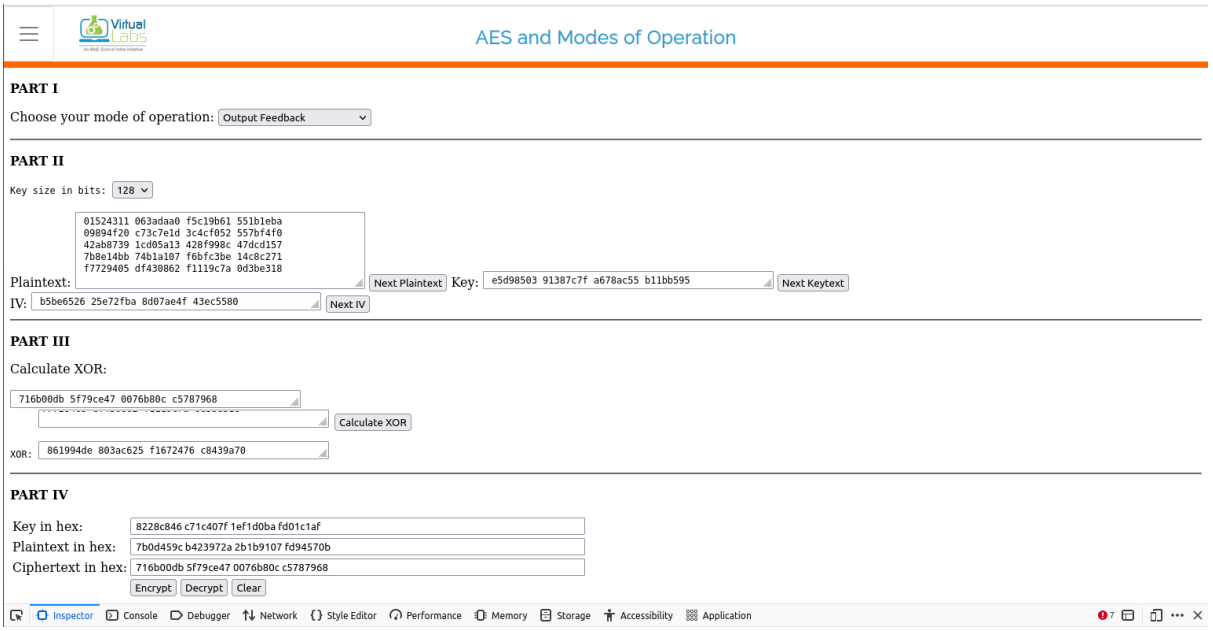
PART V

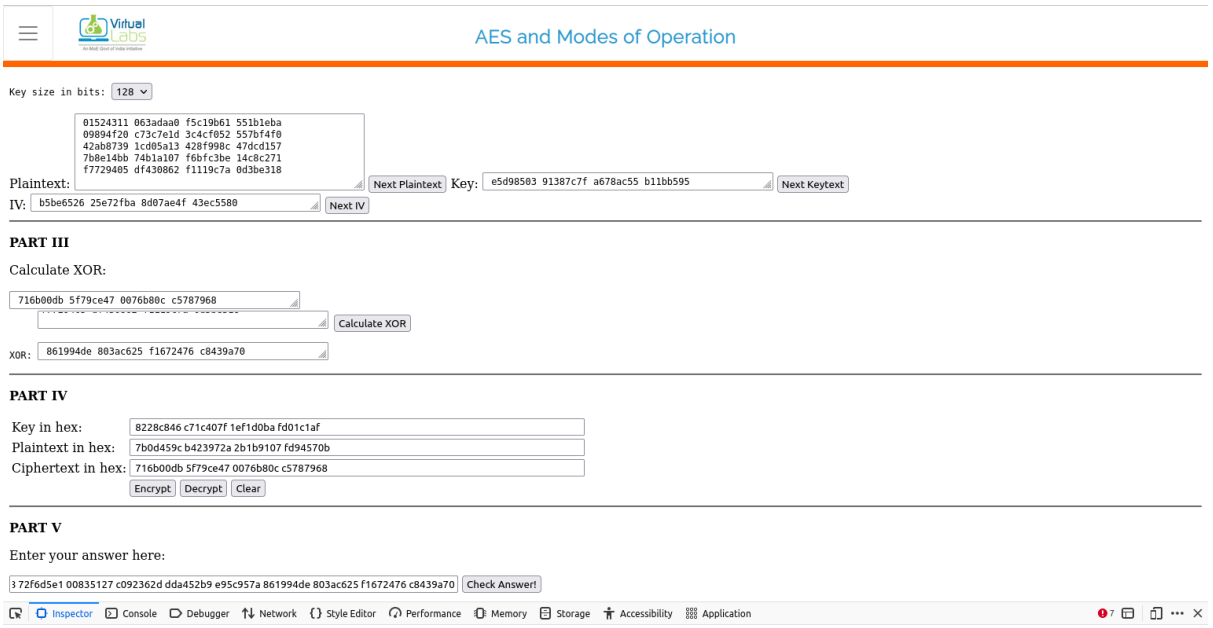
Enter your answer here:

i31 d9be843f a404bf30 def90712 715fd1de d10ae8e5 8228c846 c71c407f 1ef1d0ba fd01c1af Check Answer!

Sorry, answer is wrong. Please try again.

Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.





CONCLUSION:

Hence, I have understood the concept of AES encryption standard algorithm and its various modes and performed encryption and decryption using various modes on a virtual simulator.