Aim:
Block cipher modes of operation using Advanced Encryption Standard (AES).

LO Mapping: LO2

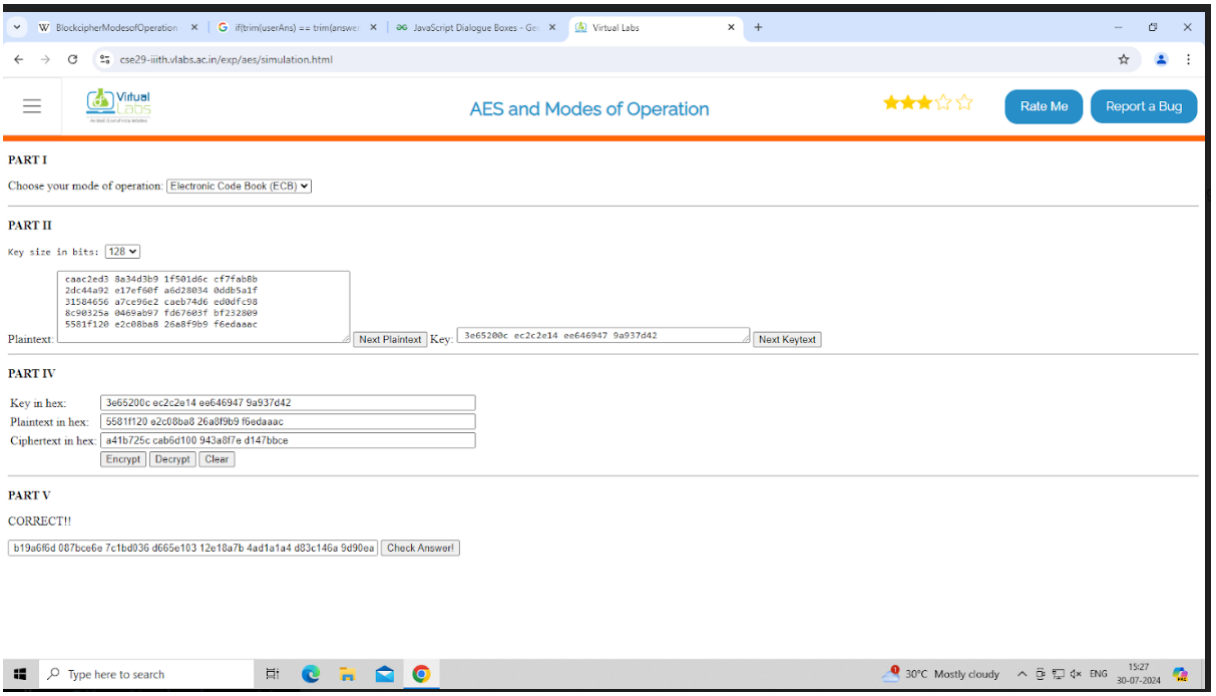
Theory & Output:

Advanced Encryption Standard (AES):

AES is a symmetric encryption algorithm used to secure data. It operates on blocks of data (128 bits) and supports key sizes of 128, 192, or 256 bits. AES is widely used due to its strength and efficiency. It involves multiple rounds of processing where each round includes substitution (using S-box), permutation (shifting rows), mixing (combining columns), and key addition steps.

Electronic Codebook(ECB)

Electronic Codebook (ECB) is a simple mode of operation for block ciphers. It encrypts each block of plaintext independently using the same encryption key.
1. Block-based: The plaintext is divided into fixed-size blocks (e.g., 64 or 128 bits), and each block is encrypted separately.
2. Independent Encryption: Each block is treated independently, meaning identical plaintext blocks will produce identical ciphertext blocks.
3. Weakness: Because of this independence, ECB does not hide data patterns well, making it vulnerable to certain types of attacks, especially when encrypting large amounts of data or highly structured data (e.g., images). Due to these weaknesses, ECB is generally not recommended for encrypting sensitive data.



Cipher Block Chaining (CBC)

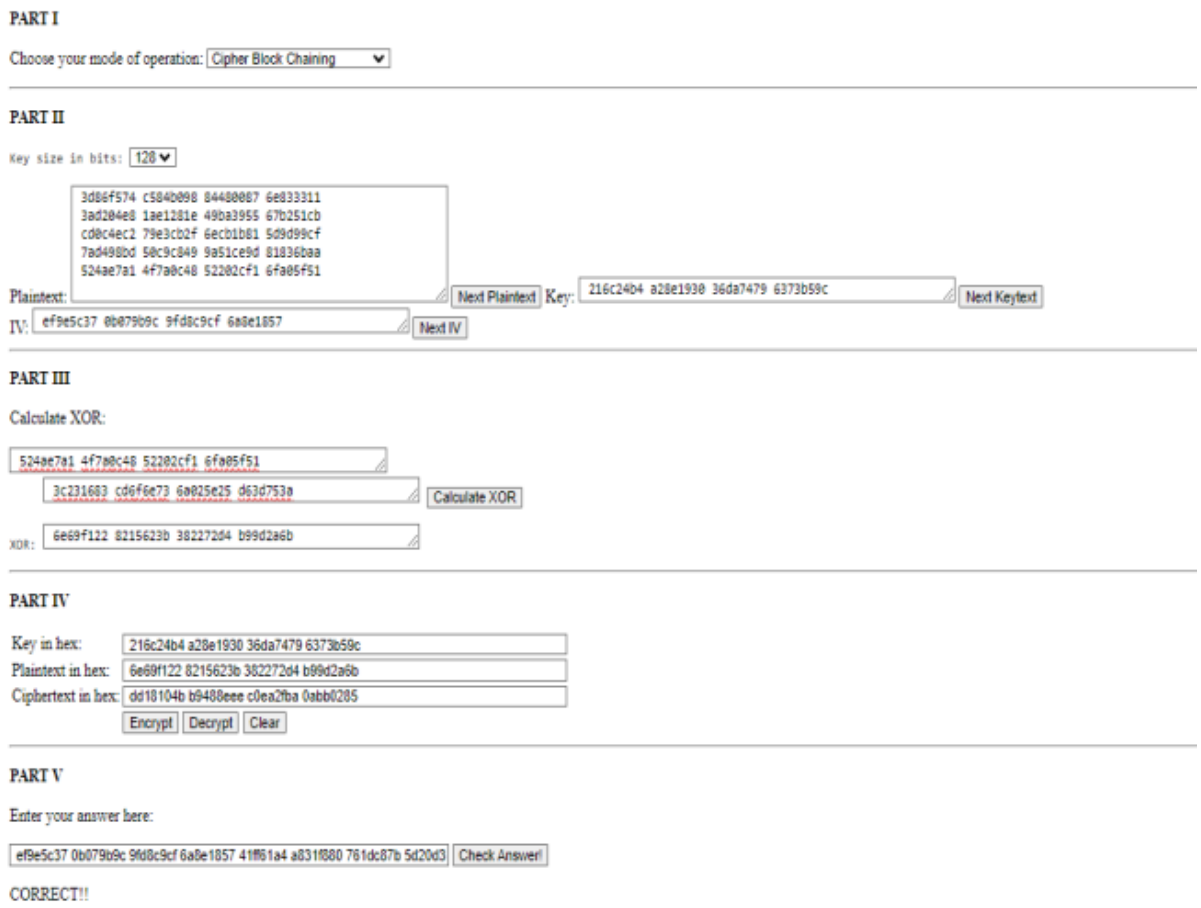
Cipher Block Chaining (CBC) is a mode of operation for block ciphers that provides enhanced security by linking the encryption of each block to the previous one.

1. Chaining: Each plaintext block is XORed with the previous cipher-text block before encryption. This means that the encryption of each block depends on the previous block, making patterns less visible in the cipher-text.

2. Initialization Vector (IV): The process starts with an IV, a random block that is XORed with the first plaintext block. This ensures that even if the same plaintext is encrypted multiple times, the resulting cipher-text will be different each time.

3. Security: The chaining mechanism helps in hiding patterns in the plaintext, making CBC much more secure than ECB. However, if an error occurs in one block, it can affect the decryption of subsequent blocks.

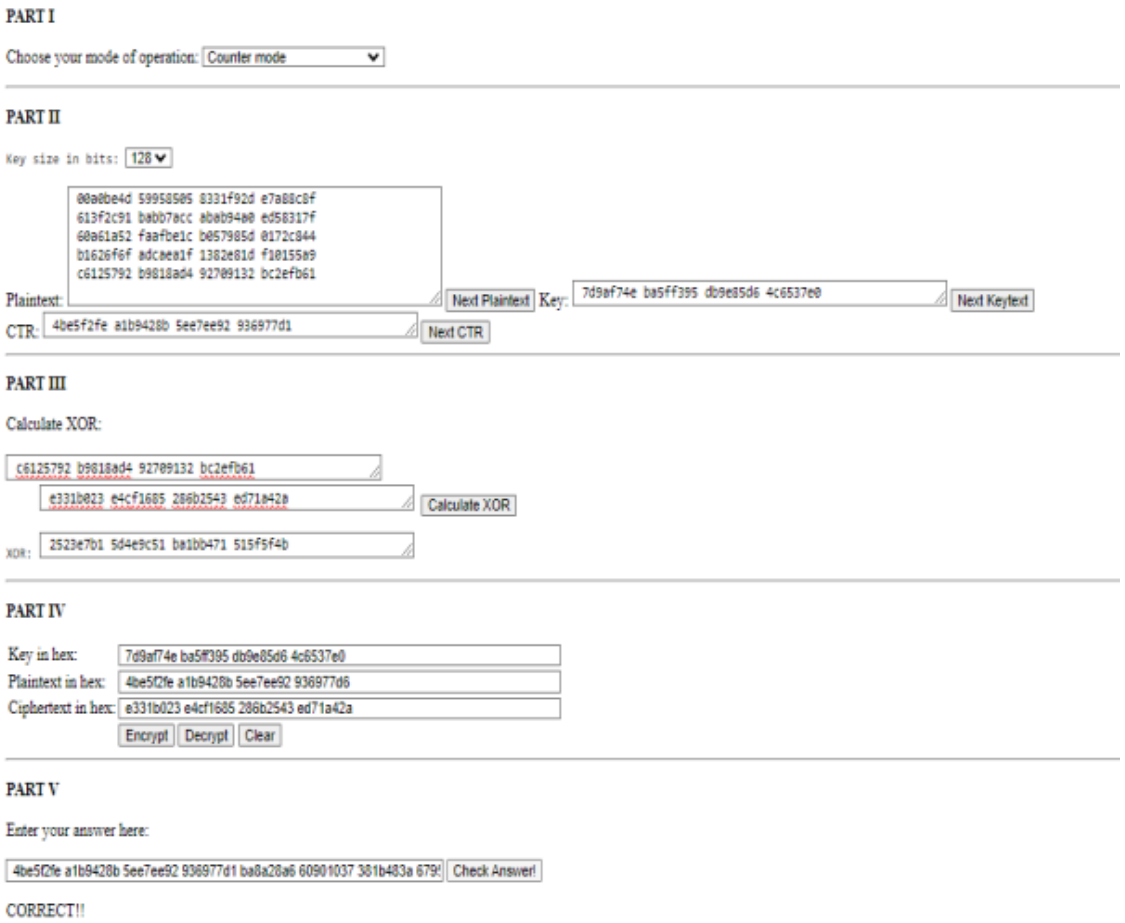
CBC is widely used in practice due to its improved security features compared to simpler modes like ECB.



Counter Mode

Counter (CTR) Mode is a mode of operation for block ciphers that turns a block cipher into a stream cipher by generating a unique key stream for each block.
1. Counter-Based: Instead of directly encrypting the plaintext, CTR mode encrypts a counter value, which is then XORed with the plaintext to produce the cipher-text. The counter is usually a simple incrementing number, ensuring that each block uses a different key stream.

2. Parallelizable: Unlike other modes like CBC, CTR mode allows for parallel encryption and decryption of blocks because the counter values are independent of the plaintext. This makes CTR mode very efficient for high-speed encryption.
3. Initialization Vector (IV): CTR mode uses an IV or a nonce to start the counter sequence, ensuring that the same plaintext encrypted multiple times will produce different cipher-texts.
4. Security: CTR mode is secure and widely used, but care must be taken to never reuse the same IV/counter combination with the same key, as it would lead to vulnerabilities. CTR mode is popular in modern encryption due to its efficiency and ability to handle parallel processing.



Output Feedback Mode

Output Feedback (OFB) Mode is a mode of operation for block ciphers that turns a block cipher into a stream cipher by generating a key stream independently of the plaintext.

1. Stream Generation: OFB mode generates a key stream by encrypting an initialization vector (IV) and then repeatedly encrypting the output of the previous encryption to produce the next part of the key stream.

2. XOR Operation: Each block of plaintext is XORed with the corresponding block of the key stream to produce the ciphertext. This makes it similar to a stream cipher.

3. No Error Propagation: Errors in one block do not affect the decryption of other blocks, making OFB mode resilient to transmission errors.

4. Initialization Vector (IV): The IV is critical in OFB mode and must be unique for each encryption session to ensure security. Reusing an IV with the same key compromises the security of the cipher.

PART I

Choose your mode of operation: Output Feedback

PART II

Key size in bits: 128

Plaintext:
```
2d4f848e d779e9e4 3135b18b c07fd150
d7a5e32c 21be3047 7fa92a4c 8adb299a
ac208bf0 5a4dc465 2d6d421b f635064d
5acfdb3f ab05908f 49e3dcf8 6f9a438d
32413a5f 96181aa0 facbb1b4 30c052c7
```
Next Plaintext Key: 954b1518 2042f8de 642504d4 bbaa5089 Next Keytext

IV: 388dec05 e8ed8799 aa26e89f 310a4831 Next IV

PART III

Calculate XOR:

32413a5f 96181aa0 facbb1b4 30c052c7

8f9b293e 7bac8928 46ba0b58 8fa61c83 Calculate XOR

XOR: bdda1361 edb49388 bc71baec bf664e44

PART IV

Key in hex:	954b1518 2042f8de 642504d4 bbaa5089
Plaintext in hex:	8f9b293e 7bac8928 46ba0b58 8fa61c83
Ciphertext in hex:	8f9b293e 7bac8928 46ba0b58 8fa61c83

Encrypt Decrypt Clear

PART V

Enter your answer here:

4b8e6401 16efb156 74e0a1f8 92df6445 35d5b985 1955ead4 ad3f7fe9 236f00b Check Answer!

Conclusion:

In conclusion, the Advanced Encryption Standard (AES) employs various block cipher modes of operation, each designed to enhance security and provide specific functionalities. These modes—such as ECB, CBC, CFB, OFB, and CTR—offer different levels of data confidentiality and integrity. Understanding the strengths and weaknesses of each mode is crucial for selecting the appropriate method for a given application, ensuring robust encryption and data protection.