

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.

W BlockCipherModesOfOperation x G if(trim(userAns) == trim(answer)) x JavaScript Dialogue Boxes - Ge x Virtual Labs

cse29-iith.vlabs.ac.in/exp/simulation.html

AES and Modes of Operation

★★★★☆ Rate Me Report a Bug

PART I

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

PART II

Key size in bits: 128

Plaintext: canc2ed3 8a34d3b9 1f501d6c cf7fab8b
2dc44a92 e17ef60f a6d28034 0ddb5a1f
31584656 a7ce99e2 caeb74d6 e0b0fc98
8c9e125a 0a09a097 f067f081f b7232809
5581f120 e2c08ba8 26a8f9b9 f6eda5ac Next Plaintext Key: 3e65200c ec2c2e14 ee646947 9a937d42 Next Keytext

PART IV

Key in hex: 3e65200c ec2c2e14 ee646947 9a937d42

Plaintext in hex: 5581f120 e2c08ba8 26a8f9b9 f6eda5ac

Ciphertext in hex: a41b725c cab6d100 943a0ff7e d147bbce

Encrypt Decrypt Clear

PART V

CORRECT!!

b19a6f6d 087bce6e 7c1bd036 d665e103 12e10a7b 4ad1a1a4 d03c146a 9d90ea Check Answer!

Type here to search 30°C Mostly cloudy 15:27 30-07-2024

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.

PART I

Choose your mode of operation: Cipher Block Chaining

PART II

Key size in bits: 128

```
3d86f574 c584b098 84480807 6e833311
3ad284e8 1ae1281e 49ba3955 67b251cb
cd8c4ec2 79e3cb2f 6ecb1b81 5d9d99cf
7ad498bd 58c9c849 9a51ce9d 81836baa
524ae7a1 4f7a8c48 52282cf1 6fa05f51
```

Plaintext:

Next Plaintext

Key:

216c24b4 a28e1938 36da7479 6373b59c

Next Keytext

IV: ef9e5c37 0b079b9c 9fd8c9cf 6a8e1857

Next IV

PART III

Calculate XOR:

524ae7a1 4f7a8c48 52282cf1 6fa05f51

3c231683 cd6f6e73 6a825e25 d63d7538

Calculate XOR

XOR: 6e69f122 8215623b 382272d4 b99d2a6b

PART IV

Key in hex: 216c24b4 a28e1938 36da7479 6373b59c

Plaintext in hex: 6e69f122 8215623b 382272d4 b99d2a6b

Ciphertext in hex: dd18104b b9488eee c0ea2ba 0abb0285

Encrypt

Decrypt

Clear

PART V

Enter your answer here:

ef9e5c37 0b079b9c 9fd8c9cf 6a8e1857 41f61a4 a831f880 761dc87b 5d20d3

Check Answer!

CORRECT!!

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.

PART IChoose your mode of operation: Counter mode**PART II**Key size in bits: 128

```
00a0be4d 59950505 0331f92d e7a80c8f
613f2c91 babb7acc abab94a0 ed58317f
60a61a52 faafb01c b057985d 0172c044
b1626f6f adcae01f 1302e81d f1015509
c6125792 b9818ad4 92709132 bc2efb61
```

Plaintext:

Next Plaintext

Key:

7d9af74e ba5ff395 db9e05d6 4c6537e0Next Keytext

CTR:

4be5f2fe a1b9428b 5ee7ee92 936977d1Next CTR**PART III**

Calculate XOR:

c6125792 b9818ad4 92709132 bc2efb61e331b023 e4cf1685 286b2543 ed71a42aCalculate XOR

XOR:

2523e701 5d4e9c51 ba1bb471 515f5f4b**PART IV**

Key in hex:

7d9af74e ba5ff395 db9e05d6 4c6537e0

Plaintext in hex:

4be5f2fe a1b9428b 5ee7ee92 936977d1

Ciphertext in hex:

e331b023 e4cf1685 286b2543 ed71a42aEncryptDecryptClear**PART V**

Enter your answer here:

4be5f2fe a1b9428b 5ee7ee92 936977d1 ba8a20a6 60901037 301b483a 679cCheck Answer!

CORRECT!!

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:

PART II

Key size in bits:

2d4f848e d779e9e4 3135b18b c07fd150
d7a5e32c 21be3047 7fa92a4c 8adb299a
ac208bf0 5a4dc465 2d6d421b f635064d
5acfdb3f ab05908f 49e3dcf8 6f9a438d
32413a5f 96181aa0 facbb1b4 30c052c7

Plaintext:

IV:

Key:

PART III

Calculate XOR:

XOR:

PART IV

Key in hex:

Plaintext in hex:

Ciphertext in hex:

PART V

Enter your answer here:

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.