

Name: Adarsh Mishra
Roll no: 104
Batch: T23

ASSIGNMENT NO 3

Aim: Encrypt long messages using various modes of operation using AES.

Electronic Code Block (ECB)

Theory:

In ECB mode, the plaintext is divided into blocks, and each block is encrypted independently using the same key. This is the simplest mode of operation for block ciphers.

Key Concepts:

- Each block of plaintext is encrypted separately.
- Identical plaintext blocks produce identical ciphertext blocks, which can reveal patterns in the data.

Example:

- Plaintext: ATTACKATDAWN
 - Blocks: ATT, ACK, ATD, AWN
 - Encrypted Blocks: E1, E2, E1, E3 (assuming E1, E2, E3 are the encrypted versions)

Cipher Block Chaining Mode (CBC)

Theory:

In CBC mode, each plaintext block is XORed with the previous ciphertext block before being encrypted. The first plaintext block is XORed with an initialization vector (IV).

Key Concepts:

- Each ciphertext block depends on all previous plaintext blocks.
- Requires an IV for the first block.
- Identical plaintext blocks result in different ciphertext blocks.

Name: Adarsh Mishra
Roll no: 104
Batch: T23

Example:

- Plaintext: ATTACKATDAWN
- Blocks: ATT, ACK, ATD, AWN
- Initialization Vector: IV
- Encrypted Blocks: C1, C2, C3, C4
- $C1 = \text{Encrypt}(\text{IV XOR ATT})$
- $C2 = \text{Encrypt}(C1 \text{ XOR ACK})$
- $C3 = \text{Encrypt}(C2 \text{ XOR ATD})$
- $C4 = \text{Encrypt}(C3 \text{ XOR AWN})$

Output Feedback Mode (OFB)**Theory:**

In OFB mode, the encryption of an IV generates a keystream, which is then XORed with the plaintext to produce the ciphertext. This keystream is independent of the plaintext and is generated before encryption.

Key Concepts:

- Converts a block cipher into a stream cipher.
- The keystream depends only on the IV and the key.
- Identical IVs produce identical keystreams.

Example:

- Plaintext: ATTACKATDAWN
- Keystream: KS1, KS2, KS3, KS4 (generated from IV and key)
- Ciphertext: C1, C2, C3, C4
- $C1 = \text{KS1 XOR ATT}$
- $C2 = \text{KS2 XOR ACK}$
- $C3 = \text{KS3 XOR ATD}$
- $C4 = \text{KS4 XOR AWN}$

Name: Adarsh Mishra
Roll no: 104
Batch: T23

Counter Mode (CTR)

Theory:

In CTR mode, a counter is encrypted to produce a keystream block, which is then XORed with the plaintext block to produce the ciphertext. The counter is incremented for each subsequent block.

Key Concepts:

- Converts a block cipher into a stream cipher.
- The counter can be any function that produces a sequence of unique values.
- Parallelizable encryption and decryption.

Example:

- Plaintext: ATTACKATDAWN
- Counter: CTR1, CTR2, CTR3, CTR4
- Keystream: KS1, KS2, KS3, KS4 (generated from encrypting the counter)
- Ciphertext: C1, C2, C3, C4
 - $C1 = KS1 \text{ XOR } ATT$
 - $C2 = KS2 \text{ XOR } ACK$
 - $C3 = KS3 \text{ XOR } ATD$
 - $C4 = KS4 \text{ XOR } AWN$

Each of these modes has its own strengths and weaknesses, and the choice of mode depends on the specific requirements and constraints of the application.

Name: Adarsh Mishra
Roll no: 104
Batch: T23

Screenshots:

Electronic Code Block (ECB)

Virtual

AES and Modes of Operation

★★★★★

Rate Me

Report a Bug

Change your mode of operation: **Electronic Code Block (ECB)**

PART II

Key size in bits: **128**

29e2c008 74452eff d01d40c a750018a
f98f5102 89c5a6a 1070889 f9a8229
16a00a4e d09e0d5 942d1c10 1c2700f3
c586e9e 5a0b0a4 9d1f5d0 8d71485
a752a307 407ab6b 22f197de 83a60600

Plaintext

Next Plaintext

Key

29e2c008 74452eff d01d40c a750018a
f98f5102 89c5a6a 1070889 f9a8229
16a00a4e d09e0d5 942d1c10 1c2700f3
c586e9e 5a0b0a4 9d1f5d0 8d71485
a752a307 407ab6b 22f197de 83a60600

Next Key

IV

Next IV

CTR

Next CTR

PART III

Calculate XOR

Calculate XOR

xor

PART IV

Key in hex: **246e75bc b3b951c7 2b7f36e4 39b6b4e4**

Plaintext in hex: **4752a307 49740e8b 2253055e 818a0660**

Ciphertext in hex: **85a14136 7560be13 8699e5b4 ef5a6bee**

Encrypt

Decrypt

Clear

PART V

Enter your answer here:

307bacc3 1030633c ddcf908a 13182375 d08966bd 29061711 0dab9034 837f194

Check Answer!

CORRECT!!

Name: Adarsh Mishra
Roll no: 104
Batch: T23

Cipher Block Chaining Mode (CBC)

The screenshot shows the 'AES and Modes of Operation' web application. The 'Key size in bits' is set to 128. The 'Plaintext' field contains a 16-byte hex string: 3d31c088 7e980208 7c00707c 0a00100a 0f3d4e79 07400501 3d8c7239 42020310. The 'Next Plaintext / Key' field contains: 77b0e000 22954010 4d52010 037000. The 'Next Key/Next' button is visible. Below this, 'PART III' 'Calculate XOR' shows the XOR of the first two plaintext blocks: 00f0a0e 04087ad 07e0100d 0010a008. 'PART IV' shows the 'Key as hex' as 77b0e000 22954010 4d52010 037000, 'Plaintext as hex' as 3d31c088 7e980208 7c00707c 0a00100a, and 'Ciphertext as hex' as 0a17b0d2 5e73b0c 004d401a 0a000a03. 'PART V' shows the 'Enter your answer here' field with the correct ciphertext: 020802 e00d01e 2a2a0e2 0019a008 0a000000 205a0dc 2207c400 7a0a0a03. The status is 'Correct!'.

Output Feedback Mode (OFB)

The screenshot shows the 'AES and Modes of Operation' web application with 'Output Feedback' mode selected. 'PART II' shows 'My size in bits' as 128. The 'Plaintext' field contains a 16-byte hex string: 0f000000 010a70ad 2a07030a c00700f 0f400000 7ad70ad 0a07030a 0a07030a 07070000 0a000000 2a07030a 0a000000 07070000 0f000000 0a000000 0a000000. The 'Next Plaintext / Key' field contains: 3d700000 01000000 4d07030a 7a070000. The 'Next Key/Next' button is visible. Below this, 'PART III' 'Calculate XOR' shows the XOR of the first two plaintext blocks: 00f0a0e 04087ad 07e0100d 0010a008. 'PART IV' shows the 'Key as hex' as 0f000000 010a70ad 2a07030a 0a07030a, 'Plaintext as hex' as 0f000000 010a70ad 2a07030a 0a07030a, and 'Ciphertext as hex' as 0a17b0d2 5e73b0c 004d401a 0a000a03. 'PART V' shows the 'Enter your answer here' field with the correct ciphertext: 0a17b0d2 5e73b0c 004d401a 0a000a03. The status is 'Correct!'.

Name: Adarsh Mishra
Roll no: 104
Batch: T23

Counter Mode (CTR)



Conclusion:

In this experiment we learnt about different modes of operations in AES and they are Electronic Code Block, Cipher Block Chaining Mode (CBC), Counter Mode (CTR), Output Feedback Mode (OFB). We also learnt to implement them.