Assignment Number: 3

Name: Archie Shah; Branch: I.T (T.E.); Roll Number: 117 25/09/2023

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

**LO mapped:** LO2

**Theory:**

AES –

The Advanced Encryption Standard (AES) is a widely used symmetric-key encryption algorithm that was established as a federal standard by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is a fundamental component of modern cryptography and is employed in a multitude of applications to secure data transmission and storage. Here's a brief theory about AES:

**AES Encryption Algorithm**

AES operates on blocks of data and employs a symmetric-key approach, meaning the same key is used for both encryption and decryption. The algorithm accepts plaintext data and transforms it into ciphertext using a series of well-defined steps. These steps involve key expansion, substitution, permutation, and mixing operations. The primary components of AES include:

1. **Key Expansion**: AES supports key sizes of 128, 192, and 256 bits. The key expansion process generates a set of round keys from the original encryption key. These round keys are used in the subsequent rounds of encryption and are derived through a combination of key scheduling and mathematical operations.
2. **Substitution**: AES employs a substitution-permutation network (SPN) structure. In the substitution step, each byte of the plaintext is replaced with a corresponding byte from a fixed substitution table called the S-box. This step introduces confusion and non-linearity into the encryption process.
3. **Permutation**: In this step, the positions of bytes within the block are rearranged. This process, known as mixing or permutation, further enhances the diffusion of data and makes it resistant to attacks.
4. **Mixing**: AES uses a series of matrix multiplication operations called MixColumns. This operation ensures that each byte in the block influences every other byte, providing additional security against various cryptographic attacks.
5. **Key Addition**: At the beginning of each round, a round key is XORed (bitwise exclusive OR) with the block of data. This step ensures that each round of encryption is dependent on both the plaintext and the round key.

**AES Decryption**

The decryption process in AES is the reverse of the encryption process. It involves reversing the operations applied during encryption, such as inverse substitution, inverse permutation, and inverse mixing. The round keys are used in reverse order during decryption.

In AES (Advanced Encryption Standard), there are several modes of operation that dictate how the encryption algorithm is applied to plaintext data to produce ciphertext. These modes determine how blocks of data are processed and how they relate to each other. Here's an explanation of some common modes of operation in AES:

1. **Electronic Codebook (ECB)**:
   * **Description**: 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.

|  |
| --- |
| Block Cipher modes of Operation - GeeksforGeeks |

* + **Advantages**: Simple and parallelizable, making it suitable for hardware implementation.
  + **Drawbacks**: Lack of diffusion (repetitive patterns in plaintext produce repetitive patterns in ciphertext), and it's not suitable for encrypting large amounts of data with the same key.

1. **Cipher Block Chaining (CBC)**:
   * **Description**: In CBC mode, each plaintext block is XORed with the ciphertext of the previous block before encryption. The initialization vector (IV) is XORed with the first plaintext block to add randomness to the process.

|  |
| --- |
| Block Cipher modes of Operation - GeeksforGeeks |

* + **Advantages**: Provides better security than ECB as it eliminates identical ciphertext blocks, and it can be used for encrypting large files.
  + **Drawbacks**: Not parallelizable due to the sequential nature of block chaining, and it requires an IV.

1. **Output Feedback (OFB)**:
   * **Description**: OFB mode turns AES into a synchronous stream cipher. It encrypts an IV to produce a keystream, which is XORed with the plaintext to produce ciphertext. It does not depend on the plaintext.

|  |
| --- |
| https://media.geeksforgeeks.org/wp-content/uploads/output-feedback-mode.png |

* + **Advantages**: Parallelizable and suitable for encrypting data of varying lengths.
  + **Drawbacks**: Error propagation (a single bit error affects the entire block), and it requires synchronization between sender and receiver.

1. **Counter (CTR)**:
   * **Description**: CTR mode transforms AES into a stream cipher by encrypting a counter value (incremented for each block) to generate a keystream. The keystream is then XORed with the plaintext.

|  |
| --- |
|  |
|  |

* + **Advantages**: Highly parallelizable, efficient for random access to data, and provides good security.
  + **Drawbacks**: Requires a unique counter for each plaintext block to avoid security issues.

**Conclusion:** By this assignment we learned various modes of operation of AES algorithm.