**Experiment 10**

**Aim** - Understanding the concepts of cryptography and guidelines for using encryption.

**Theory**-**Advanced Encryption Standard (AES)** is a symmetric block cipher that is widely used for securing data. It was established as a standard by the **National Institute of Standards and Technology (NIST)** in 2001 and is used worldwide for encrypting sensitive information, including financial transactions, government data, and personal communication.

AES has become the standard encryption algorithm due to its efficiency, security, and flexibility in handling different key lengths and block sizes. AES replaced the earlier **Data Encryption Standard (DES)**, which had vulnerabilities due to its smaller key size.

### **Overview of AES**

* **Symmetric Cipher**: AES is a **symmetric encryption algorithm**, meaning the same key is used for both encryption and decryption. This requires that the sender and receiver both possess the same secret key.
* **Block Cipher**: AES operates on fixed-size blocks of data. The block size for AES is always **128 bits** (16 bytes), meaning data is processed in chunks of 128 bits at a time.
* **Key Sizes**: AES supports three different key sizes:
  + **AES-128**: Uses a 128-bit key.
  + **AES-192**: Uses a 192-bit key.
  + **AES-256**: Uses a 256-bit key. The larger the key size, the more secure the encryption, but it also increases computational overhead.

### **AES Algorithm Process**

The AES encryption algorithm involves a series of transformations applied to the data block over multiple rounds. The number of rounds depends on the key size:

* **10 rounds** for 128-bit keys.
* **12 rounds** for 192-bit keys.
* **14 rounds** for 256-bit keys.

Each round consists of several operations, designed to obscure the relationship between the plaintext and the ciphertext, and to ensure that any attack on the cipher is computationally infeasible.

#### **Main Operations in AES**

1. **SubBytes (Substitution Layer)**:
   * Each byte of the block is replaced with a corresponding byte from a fixed **Substitution Box (S-Box)**. This S-Box is designed to provide non-linearity, making it difficult to predict the output from the input.
   * This introduces confusion in the ciphertext.
2. **ShiftRows**:
   * The rows of the block are shifted by a certain number of positions. The first row is left unchanged, the second row is shifted by one position, the third row by two positions, and the fourth by three positions.
   * This operation mixes the data across the block.
3. **MixColumns**:
   * Each column of the block is transformed using a mathematical function that combines the values in each column. This operation spreads the influence of each byte over the entire block, ensuring diffusion.
   * This step ensures that changes in one byte affect multiple other bytes in the ciphertext.
4. **AddRoundKey**:
   * In this step, the current block is XORed with a portion of the encryption key (called the **Round Key**). A different portion of the key is used for each round.
   * This introduces the key into the encryption process.

The final round of AES omits the **MixColumns** step, ensuring that the output is not excessively transformed.

#### **AES Key Expansion**

The key provided during encryption undergoes a process called **Key Expansion**, where the original key is expanded into several **Round Keys**. These keys are derived from the original key and used at each round of encryption or decryption.

### **AES Modes of Operation**

AES can be used in different **modes of operation**, which specify how encryption should be applied to larger amounts of data (since AES itself only operates on 128-bit blocks). Common modes include:

1. **Electronic Codebook (ECB)**:
   * In ECB mode, each block is encrypted independently. However, this mode is insecure for large data sets because identical plaintext blocks result in identical ciphertext blocks, leading to patterns in the encrypted data.
2. **Cipher Block Chaining (CBC)**:
   * In CBC mode, each plaintext block is XORed with the previous ciphertext block before being encrypted. This introduces dependencies between blocks, ensuring that identical plaintext blocks will result in different ciphertext blocks.
3. **Counter (CTR)**:
   * In CTR mode, a counter value is encrypted, and the result is XORed with the plaintext to produce the ciphertext. CTR mode turns AES into a stream cipher, allowing parallel encryption and decryption.
4. **Galois/Counter Mode (GCM)**:
   * GCM mode is widely used for both encryption and authentication. It combines counter mode encryption with a cryptographic hash function, ensuring data integrity and confidentiality. This mode is often used in modern communication protocols like TLS.

### **Security of AES**

AES is considered extremely secure and has been the subject of extensive cryptographic analysis. As of now, no practical attacks have been found that can break AES encryption faster than brute force. Some key points regarding AES security:

* **Brute Force**: Breaking AES encryption via brute force would require trying all possible keys. For AES-128, this would involve trying 2^128 possible keys, which is computationally infeasible with current technology. AES-192 and AES-256 provide even more security, making brute force attacks impractical.
* **Side-Channel Attacks**: AES, like other cryptographic algorithms, can be vulnerable to **side-channel attacks**, which exploit information leakage during implementation (e.g., power consumption or timing information). However, these attacks can typically be mitigated through proper implementation practices.
* **Quantum Computing**: While AES is secure against classical computers, there is concern that future **quantum computers** could weaken its security. Quantum attacks like **Grover's algorithm** could reduce the security of AES by halving the effective key size (e.g., making AES-128 equivalent to AES-64). However, AES-256 would still provide strong security against such quantum attacks.

### **Applications of AES**

AES is widely used in various domains to ensure the confidentiality of data, including:

1. **Data Encryption**: AES is used to encrypt files, databases, and communication channels to protect sensitive information.
2. **VPNs and Secure Communication**: AES is the encryption standard used in most **VPNs** (Virtual Private Networks), and secure communication protocols like **SSL/TLS** (for HTTPS).
3. **Wireless Security**: AES is part of the **WPA2** (Wi-Fi Protected Access) protocol used to secure wireless networks.
4. **Disk Encryption**: Tools like **BitLocker** (Windows), **FileVault** (macOS), and other full-disk encryption tools use AES to encrypt the contents of drives.

**Data Encryption Standard (DES)** is a symmetric-key block cipher that was widely used for data encryption from the late 1970s until the late 1990s. DES is considered one of the first encryption algorithms to be widely adopted and has played a significant role in the field of cryptography.

### **Overview of DES**

1. **Symmetric-Key Cipher**:
   * DES is a symmetric encryption algorithm, meaning it uses the same key for both encryption and decryption. Both the sender and receiver must have access to the same secret key.
2. **Block Cipher**:
   * DES operates on fixed-size blocks of data. The block size for DES is **64 bits** (8 bytes). This means that it processes data in chunks of 64 bits at a time.
3. **Key Size**:
   * DES uses a key size of **56 bits**, although the actual key input is 64 bits. The 64-bit key includes 8 parity bits, which are used for error detection, reducing the effective key length to 56 bits.

### **DES Encryption Process**

The DES algorithm consists of a series of transformations applied to the data block over **16 rounds**. Each round involves multiple operations that include permutation and substitution processes to obscure the relationship between the plaintext and the ciphertext.

#### **Main Steps in the DES Encryption Process**

1. **Initial Permutation (IP)**:
   * The 64-bit plaintext is permuted according to a fixed initial permutation table. This step rearranges the bits but does not provide security on its own.
2. **Key Generation**:
   * The original 56-bit key is used to generate 16 subkeys, one for each round. Each subkey is created using a process of permutation and shifting.
3. **Rounds**:
   * DES consists of 16 rounds of processing, where each round includes:
     + **Expansion**: The 32-bit right half of the data block is expanded to 48 bits.
     + **Key Mixing**: The expanded data is XORed with the round key (subkey).
     + **Substitution**: The XOR result is split into 8 segments of 6 bits each, and each segment is substituted using S-Boxes (Substitution Boxes) to produce a 32-bit output.
     + **Permutation**: The 32-bit output undergoes a fixed permutation.
     + **Combination**: The output is combined with the left half of the block, and the halves are swapped.
4. **Final Permutation (FP)**:
   * After the last round, the final output undergoes a last permutation that is the inverse of the initial permutation. This yields the final ciphertext.

### **Security of DES**

While DES was considered secure for many years, several vulnerabilities have emerged:

1. **Key Size**:
   * The primary vulnerability of DES is its short key length of 56 bits. With advances in computing power, it became feasible for attackers to perform brute-force attacks to try all possible keys. In the late 1990s, DES was successfully broken using distributed computing efforts.
2. **Cryptanalysis**:
   * Various cryptanalytic attacks, including differential and linear cryptanalysis, have been developed against DES, demonstrating that it is not as secure as initially thought.
3. **NIST Withdrawal**:
   * In 2005, the **National Institute of Standards and Technology (NIST)** officially withdrew DES as a standard encryption algorithm, recommending the use of more secure alternatives like **Advanced Encryption Standard (AES)**.

### **DES Variants**

In response to the vulnerabilities of DES, several variants were developed:

1. **Triple DES (3DES)**:
   * To enhance security, **Triple DES** encrypts data three times using three different keys. It applies the DES algorithm three times to each block of data, effectively increasing the key length and making brute-force attacks much more difficult.
2. **International Data Encryption Algorithm (IDEA)**:
   * IDEA was developed as an alternative to DES and offers a longer key length (128 bits) while maintaining a block size of 64 bits.

### **Applications of DES**

Despite its vulnerabilities, DES was widely used in various applications during its prime:

1. **Data Encryption**: DES was employed to secure sensitive data in various industries, including finance, healthcare, and telecommunications.
2. **Secure Communication**: DES was utilized in secure communication protocols, including those for remote access and secure file transfer.
3. **Banking Systems**: Many banking systems and ATMs used DES for securing transactions and sensitive customer data.

DES is based on the two fundamental attributes of cryptography: substitution (also called confusion) and transposition (also called diffusion). DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition. Let us now discuss the broad-level steps in DES.

**1) In the first step, the 64-bit plain text block is handed over to an initial Permutation (IP) function.**

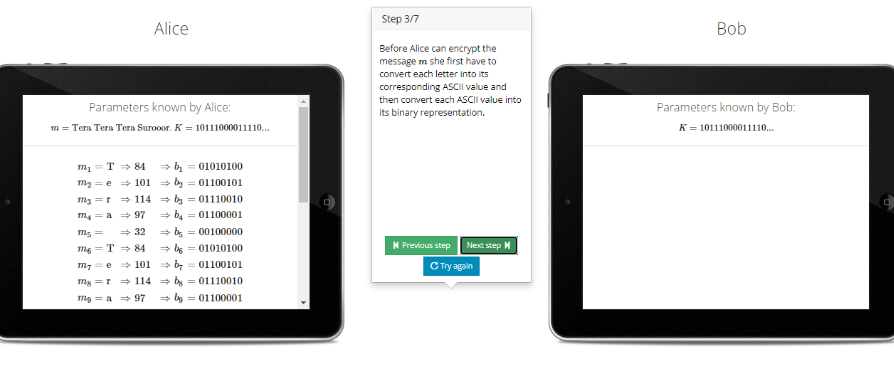
**2) The initial permutation is performed on plain text.**

**3) Next, the initial permutation (IP) produces two halves of the permuted block; saying Left Plain Text (LPT) and Right Plain Text (RPT).**

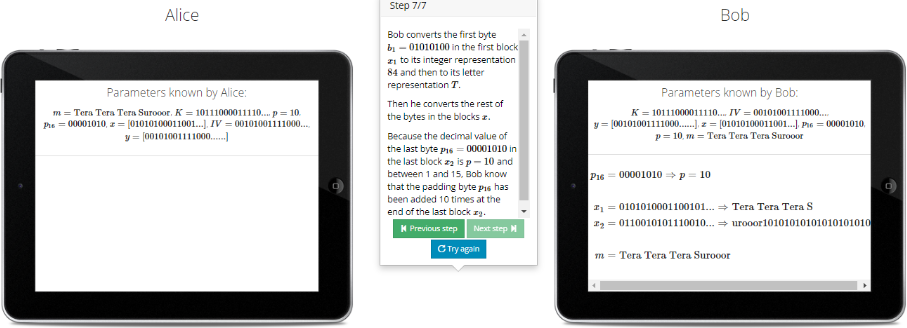
**4) Now each LPT and RPT go through 16 rounds of the encryption process.**

**5) In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block**

**6) The result of this process produces 64-bit ciphertext.**

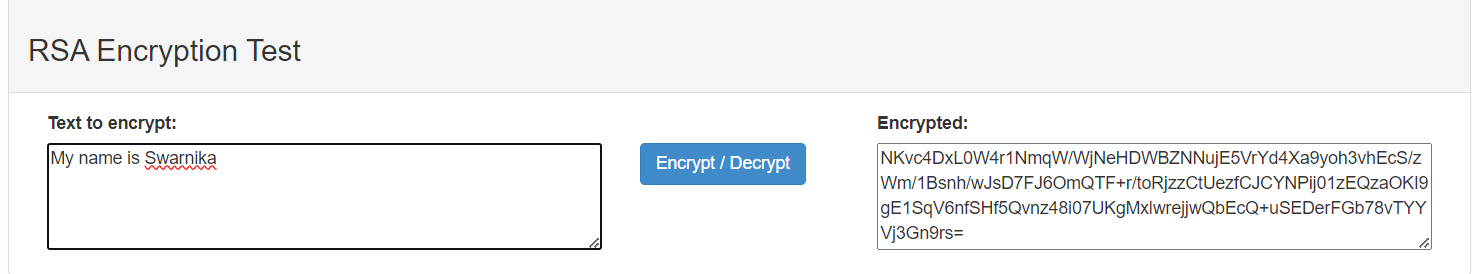












**Conclusions** :Thus we have understood the concepts of cryptography and guidelines for using encryption.