|  |  |  |  |
| --- | --- | --- | --- |
| **Course Name:** | **Applied Cryptography 116U01E628** | **Semester:** | **VI** |
| **Date of Performance:** | **12/03/25** | **DIV/ Batch No:** | **C - 3** |
| **Student Name:** | **Romil Lodaya** | **Roll No:** | **16010122096** |

**Experiment No: 6**

**Title: Understanding Symmetric Key Cryptography Algorithms (DES and AES)**

|  |
| --- |
| **Aim and Objective of the Experiment:** |
| Understanding Symmetric key cryptography algorithms (DES and AES) using  Virtual Lab: https://cse29-iiith.vlabs.ac.in |

|  |
| --- |
| **COs to be achieved:** |
| **CO2: Demonstrate and implement various Cryptographic Algorithms for securing systems.** |

|  |
| --- |
| **Books/ Journals/ Websites referred:** |
| 1. Stallings, W., Cryptography and Network Security: Principles and Practice, Second edition, Person Education 2. Forouzan, B. A. (2018). Cryptography and Network Security. McGraw-Hill Education. |

|  |
| --- |
| **Theory:** Explain the following. |
| Symmetric key cryptography:   * Symmetric key cryptography concepts: Fiestel and non-Fiestel ciphers, confusion, diffusion * The basic structure of a DES, 3DES (diagrams) * Basic structure of AES. |

|  |
| --- |
| **Code and Output :**  Refer to the virtual Labfor theory and simulation[**https://cse29-iiith.vlabs.ac.in**](https://cse29-iiith.vlabs.ac.in)  1.Screenshots: DES execution step by step    Encryption using KeyA:    Decryption using KeyB:    Encryption using KeyA:       1. Screenshots: AES execution step by step |
|  |

|  |
| --- |
| **Post Lab Subjective/Objective type Questions:** |
| 1. Compare and contrast AES/DES  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | | **Feature** | **AES (Advanced Encryption Standard)** | **DES (Data Encryption Standard)** | | --- | --- | --- | | **Key Size** | 128, 192, or 256 bits | 56 bits | | **Block Size** | 128 bits | 64 bits | | **Rounds** | 10, 12, or 14 (depending on key size) | 16 rounds | | **Algorithm Type** | Substitution-Permutation Network (SPN) | Feistel Network | | **Security Level** | Highly secure; resistant to known attacks | Weak; vulnerable to brute-force attacks | | **Speed** | Faster and more efficient | Slower compared to AES | | **Vulnerability** | No practical attacks so far | Susceptible to brute force and differential cryptanalysis | |  * **AES is more secure** due to its larger key size and improved design. * **DES is outdated** and insecure due to its small key size, making it vulnerable to brute-force attacks. * **AES is more efficient** and widely used for modern encryption applications.  1. Comment on the strengths and weaknesses of a symmetric key cryptosystem.  ****Strengths:****  1. **Efficiency** – Symmetric encryption is computationally faster than asymmetric encryption. 2. **Lower Resource Consumption** – Requires less processing power, making it suitable for real-time applications. 3. **Simplicity** – Uses the same key for encryption and decryption, making implementation straightforward. 4. **Strong Security (with Large Keys)** – When properly implemented with long keys (e.g., AES-256), symmetric encryption provides robust security.  ****Weaknesses:****  1. **Key Distribution Problem** – Securely sharing the key between sender and receiver is a major challenge. 2. **Scalability Issues** – In a large network, managing a unique key for each pair of users becomes impractical. 3. **No Authentication** – Symmetric encryption ensures confidentiality but does not provide authentication or non-repudiation. 4. **Single Point of Failure** – If the key is compromised, all encrypted data can be decrypted by an attacker. |

|  |
| --- |
| **Conclusion:** |
| AES is superior to DES in security and efficiency. Symmetric cryptosystems are fast and secure but face key distribution challenges, often requiring hybrid encryption for practical use. |