Computer Networking: Security

(CSE3752)

List of Projects

1. **Securing Remote Device Administration in an Enterprise Network using SSH and AAA Server Authentication**

Problem Statement:

In modern enterprise networks, IT administrators frequently manage networking equipment remotely. However, using insecure protocols like Telnet poses significant risks, as credentials and configuration data can be intercepted during transmission. To ensure secure administrative access, organizations adopt **SSH (Secure Shell)** for encrypted communication and implement **centralized user authentication using AAA (Authentication, Authorization, and Accounting)** servers like RADIUS. This project simulates a corporate environment where network administrators must securely access routers using SSH, and user authentication is centrally managed through a AAA server. The goal is to enhance administrative security, manage user access efficiently, and reduce the risk of unauthorized configure changes.

Objectives:

1. To configure **SSH** on a Cisco router for secure remote access.
2. To implement **AAA (Authentication, Authorization, Accounting)** using a local AAA server.
3. To restrict administrative access to the router only to authorized users.
4. To test and verify secure access using SSH from administrator PCs.

2. **Securing Departmental Access in an Office Network using Access Control Lists (ACLs)**

Problem Statement:

In a real-world office environment, different departments such as HR, Finance, and IT often share the same network infrastructure but require controlled access to resources for security and privacy. For example, HR systems may contain sensitive employee data that should not be accessible to all employees, and Finance servers might need to be protected from unauthorized access. To address these needs, network administrators implement **Access Control Lists (ACLs)** on routers to restrict and permit traffic based on IP addresses, protocols, and services. This project simulates such a scenario and demonstrates how ACLs can be used to enforce departmental boundaries and secure access within a shared office network.

Objectives:

1. To understand the purpose and types of ACLs (standard and extended).
2. To design a network with multiple subnets and devices.
3. To implement **standard ACL** to restrict traffic based on source IP addresses.
4. To implement **extended ACL** to restrict traffic based on source, destination, and protocol/port.
5. To apply ACLs on appropriate router interfaces in the correct direction (inbound/outbound).
6. To test and validate ACL rules using ping, web, or FTP traffic.
7. To simulate both **permitted and denied traffic** scenarios.

3. **Securing message using playfair encryption and developing a cryptanalysis method to recover the original message from encrypted message.**

Problem Statement:

In the field of digital communication networking it is quite important to keep the information secured during transmission. To satisfy the need classical symmetric encryption techniques are well approachable by the users at the transmitting end. One of them is the use of **play-fair ciphering** that overcomes the drawback of simple mono-alphabetic ciphering. The technique uses a 5 X 5 key matrix to encrypt the plaintext. However to make it more complex the generated **key elements can be structured in different ways (i.e. row-wise/column-wise)** instead of row-column based matrix structure to get it implemented. Further, while incorporating the modification in key matrix structure it is also required to compare and analyse the respective ciphertexts obtained. The said problem can be extended to develop a **cryptanalysis process** to recover the plaintext again assuming a possible brute force attack.

Objectives:

1. **To understand the play-fair ciphering** technique and its implementation for message encryption process**.**
2. **To modify/replace the 5 X 5 key matrix** with a row-wise structured arrangement of key elements.
3. **To modify/replace the 5 X 5 key matrix** with a column-wise structured arrangement of key elements.
4. **To make a comparative analysis between the respective ciphertexts** obtained from the implementation of modification in key structure.
5. **To develop the respective decryption process** for validating the modification made in the key matrix generation technique**.**
6. **To develop and analyse a cryptanalysis process** for recovering the plaintext without the knowledge of key matrix in the form of brute force attack.

4. **Develop a program to demonstrate the RSA cryptosystem.**

   Problem statement:

   In the field of cryptography the public key infrastructure has been widely adopted because of its computational complexity nature due to the involvement of two different keys as compared to symmetric encryption techniques. **RSA (Rivest–Shamir–Adleman) cryptosystem** is quite popular among various asymmetric/public key cryptography processes because of its multiple uses like message encryption, key exchange and source authentication. The algorithm looks simple as it uses only 3 parameters (i.e. two prime numbers and one integer used for encryption/decryption). However, it is quite important to verify the genuineness of algorithm that properly validates the input and intermediate parameters to be engaged in cryptography process. This project insist the students to focus towards inclusion of techniques (such as identification of prime no., finding modular multiplicative inverse) inside the RSA algorithm for validating different parameters involved thereof. Moreover the project also considers the plaintext characters to be inputted in the form of their ASCII value for encryption and getting back to its original form after decryption.

   Objectives:

   1. **To understand the concept of public and private key used in RSA algorithm** and its implementations for different applications.
   2. **To incorporate a function** that validates the user inputs p and q as prime numbers only**.**
   3. **To implement the Extended Euclidean Algorithm** for obtaining the modular multiplicative inverse of an integer for making a pair of encryption and decryption key.
   4. **To allow the program** to handle plaintext messages as strings by converting characters to their **ASCII values** and processing them in blocks
   5. **To convert the ciphertext in to plaintext** message in its original form after decryption.

5. **Image encryption and decryption using DES.**

   ## Problem Statement:

   With the rapid advancement of digital technologies and the widespread use of multimedia data, ensuring the security of digital images has become a critical concern. Images transmitted over public or unsecured networks are vulnerable to unauthorized access, tampering, and data theft. Traditional encryption algorithms are often optimized for textual data and may not be directly applicable or efficient for image files due to their large size and different data structures. This project focuses on using the **Data Encryption Standard (DES)** algorithm—a symmetric key encryption method—to **encrypt and decrypt image files**. The aim is to ensure **confidentiality and integrity of image data** during transmission or storage, thus demonstrating the effectiveness of DES in multimedia data protection.

Objectives:

1. **To study and understand the DES (Data Encryption Standard) algorithm** and its applicability to image encryption.
2. **To develop a software system** that can encrypt a given digital image using DES, transforming it into an unreadable format.
3. **To implement a decryption module** that can accurately reconstruct the original image from its encrypted version using the correct key.
4. **To ensure the image retains its original quality and resolution** after decryption, confirming the correctness of the algorithm.
5. **To evaluate the performance of DES** in terms of encryption/decryption speed, data integrity, and resistance to basic attacks.
6. **To compare the original and decrypted images** to validate the success and reliability of the encryption process

6. Secure message encryption and decryption using Triple DES.

Problem Statement:

In today's digital age, secure communication is a critical requirement across all domains, including banking, healthcare, and personal messaging. With the growing threats of data breaches, message tampering, and unauthorized access, there is a pressing need for robust encryption mechanisms to protect sensitive information. While the Data Encryption Standard (DES) was once widely used, its vulnerabilities have led to the adoption of stronger encryption methods. **Triple DES (3DES)** enhances DES by applying the encryption process three times, providing significantly improved security. This project aims to **design and implement a system for secure message encryption and decryption using the Triple DES algorithm**, ensuring data confidentiality and resistance to brute-force attacks during communication or storage.

Objectives:

1. **Understand the working principles of the Triple DES encryption algorithm** and its advantages over standard DES.
2. **Develop a secure system** that enables users to input a plaintext message and encrypt it using the Triple DES algorithm.
3. **Implement a decryption module** that accurately retrieves the original message from the encrypted text using the correct key.
4. **Ensure data confidentiality and integrity** during encryption and decryption by handling keys securely.
5. **Evaluate the system's performance** in terms of encryption/decryption speed, accuracy, and security strength.
6. **Compare Triple DES with other symmetric encryption algorithms** (optional, for added depth), such as AES, to highlight its use cases and limitations.

7. **Image encryption and decryption using AES.**

Problem Statement:

In the current era of digital communication, the exchange and storage of image data have become commonplace in various sectors such as healthcare, defense, and social media. However, the ease of transmission over open networks also exposes image data to potential security threats such as unauthorized access, data interception, and tampering. To protect sensitive visual information, robust encryption mechanisms are required. The **Advanced Encryption Standard (AES)** is a widely accepted symmetric key encryption algorithm known for its speed, reliability, and high level of security. This project aims to **design and implement an image encryption and decryption system using the AES algorithm** to ensure the **confidentiality, integrity, and security of image data** during transmission and storage.

Objectives:

1. **To study the AES (Advanced Encryption Standard) algorithm** and understand its suitability for image data encryption.
2. **To develop a system that can encrypt a digital image using AES**, rendering it unreadable without the appropriate decryption key.
3. **To implement a decryption module** that accurately restores the original image from its encrypted version using the AES decryption process.
4. **To maintain the quality and integrity of the original image** after decryption, ensuring no significant data loss or distortion.
5. **To evaluate the performance of the AES algorithm** in terms of encryption and decryption time, security strength, and resistance to attacks.
6. **To demonstrate the practical feasibility** of using AES for securing image data in real-world applications.

8. **Secure messaging application with end to end encryption using DES and RSA.**

Problem Statement:

In today's digital landscape, the need for secure communication is more critical than ever due to the increasing risks of data breaches, eavesdropping, and unauthorized access. Messaging platforms, in particular, are common targets for cyberattacks because they often carry sensitive personal and business information. End-to-end encryption (E2EE) is a crucial solution that ensures only the communicating parties can read the messages, even if the transmission medium is compromised. This project proposes the development of a **secure messaging application that integrates both symmetric (DES) and asymmetric (RSA) encryption techniques**. The RSA algorithm will be used to **securely exchange the DES keys**, which will then be used for **fast and efficient message encryption and decryption**. This hybrid approach aims to combine the speed of DES with the key distribution security of RSA to deliver a robust end-to-end encrypted communication system.

Objectives:

1. **To study and analyze the DES and RSA encryption algorithms** and understand their strengths and weaknesses in the context of secure communication.
2. **To design and implement a secure messaging application** that supports real-time encrypted communication between users.
3. **To use RSA for secure key exchange**, ensuring that the DES encryption key is safely transmitted over the network.
4. **To implement DES for the actual message encryption and decryption**, ensuring fast and efficient performance.
5. **To ensure complete end-to-end encryption**, such that messages remain secure during transmission and cannot be intercepted or read by unauthorized parties.
6. **To evaluate the performance of the hybrid encryption model** in terms of security, speed, and reliability.

9. Secure file sharing system using DES and Diffie-Hellman algorithm.

Problem Statement:

As digital file sharing becomes increasingly common in both personal and professional contexts, the risk of unauthorized access, data interception, and cyberattacks has grown significantly. Sharing files over unsecured networks can expose sensitive data to malicious actors. Ensuring confidentiality, integrity, and secure key exchange is critical for protecting this data. While symmetric encryption algorithms like **DES** (Data Encryption Standard) offer efficient file encryption, they require a secure method for key exchange. The **Diffie-Hellman key exchange algorithm** provides a solution for securely establishing a shared secret key over an insecure channel. This project aims to **develop a secure file sharing system that integrates DES for data encryption and Diffie-Hellman for secure key exchange**, thereby ensuring that files can be shared confidentially and safely over public or private networks.

Objectives:

1. **To understand the working principles of DES and Diffie-Hellman algorithms**, including their roles in encryption and secure key exchange.
2. **To develop a secure file sharing application** that allows users to share files over a network while protecting their contents.
3. **To implement DES encryption for securing the contents of files**, ensuring data confidentiality during transmission and storage.
4. **To use the Diffie-Hellman algorithm to securely generate and exchange encryption keys**, removing the need to transmit keys directly.
5. **To ensure the shared files are decrypted correctly and without data loss**, validating the effectiveness of the encryption-decryption process.
6. **To evaluate the performance of the system** in terms of encryption speed, key exchange time, and overall data security.

10. Secure E-mail communication with proper authentication using RSA and AES.

Problem Statement:

In an era where digital communication is fundamental to personal, professional, and governmental operations, ensuring the **security and authenticity of messages** is of paramount importance. E-mail communication is one of the popular message exchange system between two distantly positioned parties using internet. Common threats such as message tampering, interception, and impersonation can lead to serious privacy breaches and loss of sensitive data. A secure communication system must not only **protect the confidentiality of the message** but also **verify the authenticity of the sender**. This project aims to develop a **secure E-mail communication system using AES for data encryption and RSA for authentication and key exchange**. AES (Advanced Encryption Standard), being a fast and secure symmetric encryption algorithm, ensures message confidentiality, while RSA (Rivest–Shamir–Adleman), an asymmetric encryption algorithm, is used for **secure key exchange and digital signatures to authenticate the sender**. Together, they provide a robust, end-to-end secure communication system.

Objectives:

1. **To study and understand the AES and RSA algorithms**, focusing on their roles in encryption, key management, and authentication.
2. **To implement AES for encrypting and decrypting messages**, ensuring the confidentiality of communication.
3. **To use RSA for secure key exchange and digital signatures**, enabling authentication and integrity verification.
4. **To design a mechanism for verifying sender identity** using RSA-based digital signatures.
5. **To develop a complete communication system** that supports secure, authenticated messaging between users.
6. **To evaluate the system's effectiveness** in terms of encryption speed, security level, and resistance to attacks such as man-in-the-middle or impersonation.