Encryption & Decryption Using Diffie Hellman Algorithm

A Project Report Submitted

to

MANIPAL ACADEMY OF HIGHER EDUCATION

BACHELOR OF TECHNOLOGY

in

Information Technology

Submitted by

Harshit Gupta – 225811376

Prabhpreet Singh Sidana - 225811286

For

The course "Information Security LabtLab"

MANIPAL INSTITUTE OF TECHNOLOGY

BENGALURU

(A constituent unit of MAHE, Manipal)

DEPARTMENT OF INFORMATION TECHNOLOGY

November 2024

DECLARATION

I hereby declare that the project work entitled **Encryption & Decryption Using Diffie Hellman Algorithm** is original and has been carried out at for the course "Software Project Management", under the guidance of **Dr. Abhijit Das.** I further declare that the work reported in this document has not been submitted either in part or full to any other Institute/University for the award of any other degree.

Harshit Gupta & Prabhpreet Singh Sidana

SIGNATURE OF THE FACULTY

(Dr.Abhijit Das)

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to Dr. Abhijit Das for his invaluable guidance, encouragement, and insightful feedback throughout this project. His expertise in information security and cryptography greatly enhanced my understanding and motivated me to explore the depths of encryption and decryption methodologies. This project, focused on implementing secure communication using the Diffie-Hellman algorithm, would not have been possible without his continued support and advice.

I am also grateful to my peers and mentors in the IS lab for their assistance and constructive suggestions, which helped in refining my approach and overcoming challenges. Their support was instrumental in completing this project, and I am truly appreciative of their collaboration and camaraderie.

ABSTRACT

The abstract is brief synopsis of the project work and should be written in 4 paragraphs. The first paragraph should introduce the area of the topic and give importance of the work / topic in the present day scenario, hence leading to the objective of the project work. The second paragraph should briefly discuss the methodology that was adopted in the work. The third paragraph should discuss briefly the important results that were obtained and its significance. The fourth paragraph should discuss the important conclusion(s) of the project work. If you have used some software tools/packages or hardware/systems, indicate them in the last line. (The abstract should fit in one page only)

Table of Contents

CHAPTER 1
INTRODUCTION

Background

The need for secure communication is paramount in the digital age, where sensitive information is transmitted over potentially insecure networks. Diffie-Hellman, a foundational cryptographic protocol, provides a way for two parties to securely generate a shared secret key over a public channel, allowing them to encrypt and decrypt messages without prior knowledge of each other's keys.

Objectives

The main objective of this project is to implement a secure key exchange system using the Diffie-Hellman algorithm, followed by encryption and decryption of messages using the derived shared key. The project aims to:

Demonstrate the Diffie-Hellman key exchange mechanism.

Implement symmetric encryption (AES) for secure message transmission.

Explore key derivation techniques to enhance security.

Scope

This project covers the implementation of Diffie-Hellman for secure key exchange and AES for encryption and decryption, demonstrating the principles of secure communication. The project does not focus on advanced cryptographic attacks or post-quantum cryptography.

CHAPTER 2
LITERATURE REVIEW

Overview

Diffie-Hellman, proposed by Whitfield Diffie and Martin Hellman in 1976, marked the first practical method for public key exchange, paving the way for modern cryptography. Existing cryptographic protocols like RSA and elliptic-curve cryptography (ECC) build upon similar principles of secure key exchange, but Diffie-Hellman remains a preferred choice for its simplicity and effectiveness in secure communications.

Key Theories and Concepts

- **Modular Arithmetic**: The security of Diffie-Hellman is based on the difficulty of solving discrete logarithm problems in large prime fields.
- **Symmetric Key Encryption (AES)**: After a shared key is established, AES is used for symmetric encryption, which is faster and well-suited for secure communication.
- **Key Derivation Functions (HKDF)**: HKDF is used to transform the shared secret into a secure cryptographic key suitable for encryption.

CHAPTER 3
METHODOLOGY

Approach

The project consists of two main components:

1. **Key Exchange**: Using the Diffie-Hellman algorithm to generate a shared secret key between two parties over an insecure channel.
2. **Encryption and Decryption**: Using AES with the derived key to encrypt and decrypt messages securely.

Tools and Technologies

- **Python**: The primary language used for implementing the algorithm.
- **cryptography Library**: Used for AES encryption, HKDF key derivation, and secure random number generation.
- **secrets Module**: Employed for generating secure random numbers.

Data Collection

No external data was gathered; the project is algorithm-based and uses generated keys and messages for demonstration.

CHAPTER 4
IMPLEMENTATION DETAILS & RESULT ANALYSIS

Project Development

1. **Key Generation**: Each party generates a private key (a random number) and a public key derived from the generator and prime number.
2. **Shared Secret Computation**: Both parties use each other's public keys with their private keys to compute a shared secret.
3. **Key Derivation (HKDF)**: The shared secret is transformed into a cryptographic key suitable for AES encryption.
4. **Message Encryption and Decryption**: Messages are encrypted with AES in CBC mode, then decrypted using the same derived key.

Key Components

- **Key Exchange Process**: Diffie-Hellman key exchange steps are implemented to generate a shared key.
- **AES Encryption/Decryption**: AES in CBC mode is implemented for secure communication.
- **Loop for Continuous Encryption**: The program allows continuous message encryption until the user exits.

Challenges and Solutions

- **Secure Key Length Adjustment**: The shared secret was initially not the correct length for AES. We resolved this by using HKDF to derive a fixed-length key.
- **Padding for AES**: AES requires messages to be block-aligned, which was managed by adding padding before encryption and removing it after decryption.

CHAPTER 5
Results and Discussion

Outcomes

The project successfully demonstrates secure key exchange using the Diffie-Hellman algorithm and encrypts messages using AES with the derived shared key. The continuous encryption loop functions as expected, allowing repeated secure message transmissions.

Analysis of Results

- **Key Exchange Validation**: The shared keys generated by both parties were identical, confirming the successful implementation of Diffie-Hellman.
- **Encryption Accuracy**: Encrypted messages could be decrypted accurately, showing that the derived key was consistent for both encryption and decryption.
- **Security Evaluation**: The use of HKDF to derive a key from the shared secret enhances security by ensuring the key is fixed-length and suitable for AES.

Comparison with Expected Results

The results align with the objectives, demonstrating successful encryption and decryption with the derived key. Expected behavior, including successful shared key generation and message confidentiality, was achieved.

REFERENCES

- Diffie, W., & Hellman, M. (1976). "New Directions in Cryptography," IEEE Transactions on Information Theory, 22(6), 644–654.
- “Cryptography Library Documentation.” Accessed October 2024.
- Menezes, A.J., van Oorschot, P.C., & Vanstone, S.A. "Handbook of Applied Cryptography." CRC Press, 1996.