ABSTRACT ALGEBRA

A Seminar Report

for course presentation of Cryptography

in partial fulfillment of requirements for the award of degree

Masters of Technology

in

Computer Science and Information Security

by

Md Firoz Alam (2023PIS5097)

Praveen Gopal Gonkar (2023PIS5112)

Saurav Kausik Mahapatra (2023PIS5119)

Akash Sindhi (2023PIS5180)

Kamal (2023PIS5182)

to

Dr. Meenakshi Tripathi

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
MALAVIYA NATIONAL INSTITUTE OF TECHNOLOGY
JAIPUR
November 2023

Abstract

Abstract algebra plays a fundamental role in modern cryptography, providing the theoretical framework for designing secure and robust cryptographic systems. This abstract explores the significance of abstract algebra in cryptography, focusing on its application in key exchange protocols and cryptographic algorithms. The use of algebraic structures such as groups, rings, and fields enables the formulation and analysis of mathematical problems that form the basis of cryptographic security. Specifically, this abstract discusses how abstract algebra underlies the Diffie-Hellman key exchange protocol and other cryptographic schemes. The elegant utilization of algebraic concepts contributes to the development of cryptographic systems that resist attacks and ensure the confidentiality, integrity, and authenticity of sensitive information.

Contents

Chapter 1

Introduction

The Diffie-Hellman algorithm is a method for securely exchanging cryptographic keys over insecure channels without compromising the security and integrity of data transmission. It was developed and published in 1976 by Martin Hellman and Whitefield Diffie. Until you received the asymmetric encryption algorithms that never relied on any category of key exchange, symmetric encryption was the only way to communicate securely. A secure method to exchange the private keys for this brand of cryptography was much needed.

Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical means, such as paper key lists transported by a trusted courier. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric-key cipher.

Diffie–Hellman is used to secure a variety of Internet services. However, research published in October 2015 suggests that the parameters in use for many DH Internet applications at that time are not strong enough to prevent compromise by very well-funded attackers, such as the security services of some countries.

Chapter 2

Literature Review

New Directions in Cryptography: Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems [1], which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

Research on Diffie-Hellman Key Exchange Protocol: This paper [2] analyzes the security of the Diffie-Hellman key exchange protocol. The purpose of the Diffie-Hellman protocol is to enable two users to exchange a secret key securely that can then be used for subsequent encryption of messages. The protocol itself is limited to the exchange of the keys. But because of having no entity authentication mechanism, the Diffie-Hellman protocol is easily attacked by the man-in-the-middle attack and impersonation attack in practice. In this paper, the computational efficiency of various authentication methods is compared. Finally, an improved key exchange schema based on a hash function is given, which improves the security and practicality of the Diffie-Hellman protocol.

An Approach to Public-Key Cryptography using Diffie-Hellman Key Exchange Algorithm: This paper [3] is an effort to solve a serious problem in Diffie-Hellman key exchange, that is, the Man-in-Middle attack. In this paper, the RSA algorithm is used along with Diffie-Hellman to solve the problem. The Man-in-Middle attack is explored, and countermeasures against the attack are analyzed.

Algebraic Generalization of Diffie–Hellman Key Exchange: This paper [4] suggests an algebraically generalized Diffie–Hellman scheme (AGDH) that, in general, enables the application of any algebra as the platform for key exchange. The underlying computational problems are formulated in the framework of average-case complexity, and the scheme is shown to be secure if the problem of computing images under an unknown homomorphism is infeasible. The paper also presents a brief survey on the algebraic properties of existing key exchange schemes and identifies the source of commutativity and the family of underlying algebraic structures for each scheme.

Chapter 3

Diffie hellman key exchange Algorithm

Step 1: Choose Prime Number and Primitive Root

- Choose a prime number q.
- Select a primitive root α of q.

Figure 3.1

Step 2: Generate Key Pairs

For the Sender

- Assume the private key for the sender as X_a where $X_a < q$.
- Calculate the public key as $Y_a = \alpha^{X_a} \bmod q$.
- Sender's key pair: $\{X_a, Y_a\}$.

For the Receiver

- Assume the private key for the receiver as X_b where $X_b < q$.
- Calculate the public key as $Y_b = \alpha^{X_b} \bmod q$.
- Receiver's key pair: $\{X_b, Y_b\}$.

Figure 3.2

Step 3: Generate Secret Key

For the Sender

- To generate the final secret key, use the private key X_a, the receiver's public key Y_b, and the prime number q.
- Calculate the key as $K = (Y_b)^{X_a} \bmod q$.

For the Receiver

- To generate the final secret key, use the private key X_b, the sender's public key Y_a, and the prime number q.
- Calculate the key as $K = (Y_a)^{X_b} \bmod q$.

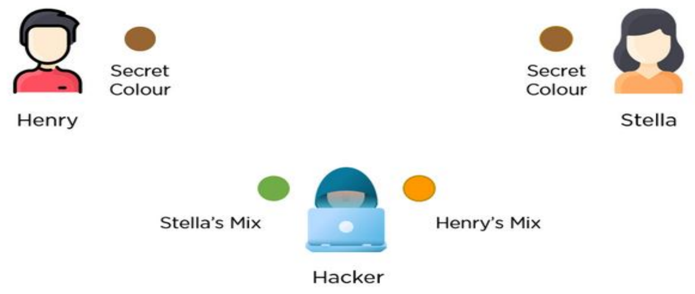

Figure 3.3

Completion Check

- If both values of K generated are equal, the Diffie-Hellman key exchange algorithm is complete.

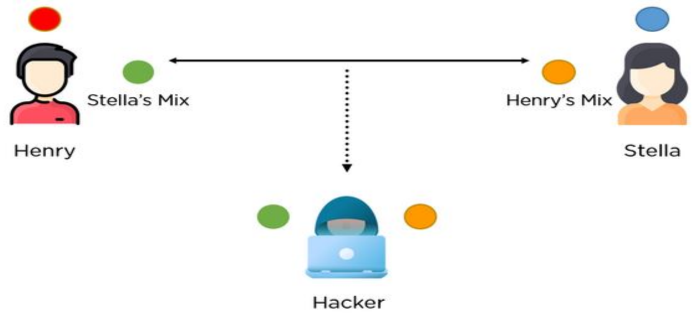

Figure 3.4

Chapter 4

Applications of Diffie Hellman Algorithm

Public Key Infrastructure (PKI)

The public-key infrastructure (PKI) is a set of tools and rules to enforce public key cryptography with multiple entities. It also governs the issuance of digital certificates over the internet to maintain data confidentiality. With the Diffie-Hellman algorithm as the base, the PKI system was created to enable the exchange of public keys with anyone who requests for it and has the appropriate permissions.

SSL/TLS Handshake

The SSL/TLS handshake is a process where internet browsers are authenticated with website servers using SSL/TLS certificates and various keys. This secure exchange of cryptographic entities over all channels is made possible by the Diffie-Hellman algorithm, ensuring the confidentiality and integrity of the communication.

Secure Shell Access (SSH)

SSH, a cryptographic protocol, is used to access system terminals from a third-party appliance or application. The Diffie-Hellman algorithm plays a crucial role in SSH by facilitating the secure exchange of keys between both systems before enabling remote access. This ensures the confidentiality and security of the communication between the user and the system.

Chapter 5

Conclusion

Abstract algebra plays a pivotal role in the Diffie-Hellman key exchange protocol, providing the mathematical foundation for its security. The protocol's reliance on abstract algebraic concepts, particularly the discrete logarithm problem in finite groups, underscores its robustness in cryptographic systems. By leveraging the algebraic properties of finite groups, the protocol enables secure key exchange, allowing parties with no prior interaction to establish a shared secret key. The elegance of the Diffie-Hellman protocol lies in its adept use of abstract algebra to address computational complexity, making it a compelling example of how theoretical mathematics can fortify the foundations of secure communication. The widespread adoption of the protocol in diverse applications highlights the enduring impact of abstract algebraic principles in modern cryptography.

References

[1] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[2] N. Li, “Research on diffie-hellman key exchange protocol,” in *2010 2nd International Conference on Computer Engineering and Technology*, vol. 4, 2010, pp. V4–634–V4–637.

[3] M. S. Rao, K. V. Rao, and M. H. M. K. Prasad, “Hybrid security approach for database security using diffusion based cryptography and diffie-hellman key exchange algorithm,” *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 1608–1612, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:245388313

[4] J. Partala, “Algebraic generalization of diffie–hellman key exchange,” *Journal of Mathematical Cryptology*, vol. 12, pp. 1 – 21, 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:42056828