MODELING DIFFIE HELLMAN KEY EXCHANGE ALGORITHM USING OBJECT-ORIENTED ANALYSIS AND DESIGN TECHNIQUE

Ashioba, Nwanze Chukwudi[1], Emma-Osiebe Obaro[2], Ogbodhu, Charles Uzoma-Odoji-Kpasa[3], Ndubuife Nonso Daniel[4]

[1]Dennis Osadebay University AnwaiAsaba, Delta State, Nigeria
[2]Delta State polytechnic Ogwashi-uku, Delta State, Nigeria
[3]Michael & Cecilia Ibru University, Delta State, Nigeria
[4]National Open University of Nigeria.

ABSTRACT

In a communicating system, information transmitted from one location (sender) to another (receiver) is secured or protected from unauthorized users or intruders. Many cryptographic algorithms have been used to prevent and protect data and information from being hacked by intruders. Both symmetric and asymmetric algorithms have not been successful in simulating cryptosystems as real-world issues with things enclosed in properties and procedures. This research simulates the Diffie Hellman key exchange algorithm using object-oriented analysis and design techniques. The researchers used the Unified Modeling Language tools in the analysis and design of the system and implemented the Diffie Hellman key exchange algorithm using C++ object-oriented programming language. The outcome demonstrates that cryptosystems are actual issues with entities having encapsulated properties and functions.

KEYWORDS

Asymmetric cryptography, Cryptography, public key, private key and symmetric cryptography

1. INTRODUCTION

Data and information in a communication system are always exposed to risks and attackers when transmitted from one location to another. The security of these data and information can be achieved by different cryptographic algorithms. [1] described cryptography as a method for verifying the integrity and confidentiality of data in a communication system. Cryptography was derived from the Greek origin “kryptos” meaning hidden and “graphy” meaning written word[2]. It is a technical method of encoding messages to prevent hackers from reading them. Cryptography is a scientific method of altering information to prevent attacks[3]. In general terms, cryptography is the technique and method of data encryption to avoid intrusion across unreliable communication routes [4], [5]. It mainly uses the mathematical principle that generates various algorithms called cryptographic algorithms [6]. To encrypt and decrypt information, a mathematical function known as a cryptographic algorithm, or cipher is used. The algorithm and a key are used to encrypt the plaintext [7]. In this context, cryptosystem refers to the collection of cryptographic techniques and the key control procedure that permits the usage of the algorithms in each application setting [7]. The two kinds of cryptographic techniques are symmetric and public key [8], [9]. In symmetric cryptography, also known as classical cryptography, the communicating parties share the same encoding/decoding key [8].Thus, the communicating parties need to agree on a unique key before utilizing a symmetric key cryptographic technique.

For symmetric key cryptography to function properly, both the sender and the recipient of the communications must be aware of and employ the same secret key when communicating [9]. The architecture of the symmetric cryptography is depicted in Figure 1.

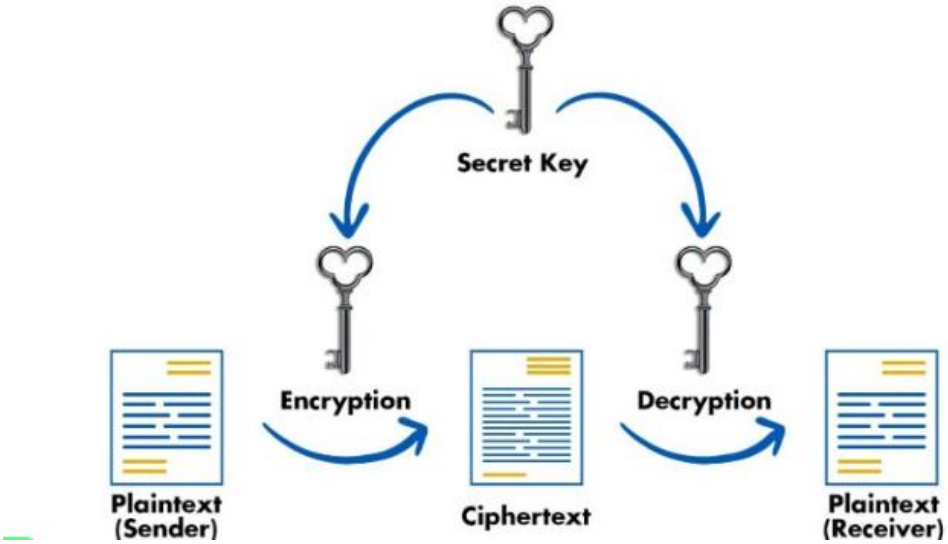

Figure 1: Symmetric key cryptography

Establishing a consensus on a single secret key that only the people involved know is the challenge with symmetric key cryptography. In 1977, Whitefield Diffie and Martin Hellman released an article proposing a key exchange system as a solution to this issue, offering the first workable solution. With the Diffie-Hellman key exchange protocol—named after them—two parties can converse over an open channel and ascertain a shared secret key without exchanging any secret keying information beforehand [9].

In asymmetric key cryptography or cryptosystems, different keys are utilised for encryption and decoding [8].

Figure 2 depicts the asymmetric key cryptosystem.

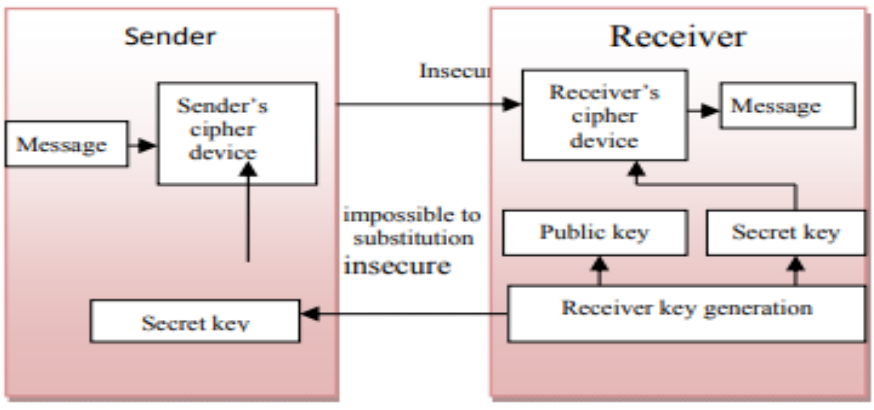

Figure 2: Structure of Asymmetric encryption scheme

The keys in this case are related to one another mathematically. The asymmetric key cryptosystem, sometimes referred to as the public key cryptosystem, encrypts and decrypts

information using both private and public keys. Each user's public key is kept secret by maintaining the confidential nature of their private key, which stops the communication parties from exchanging or revealing sensitive data (keys). Because they offer the advantages of confidentiality and authentication, public key cryptosystems are the most widely used.

2. DIFFIE-HELLMAN KEY EXCHANGE

The Diffie-Hellman key exchange, often known as the exponential key exchange, is a method for securely sending cryptographic keys across an erratic channel. It is acrucial component of several secure communication protocols, such as SSH, TLS, and SSL. A breakthrough in public key cryptography was the Diffie-Hellman key exchange, which allows two parties to securely generate a secret key for communication security. Diffie-Hellman protocols for authenticated key exchange were developed by [10]. The protocol established a shared secret key for a group of players, ensuring multicast integrity. Over time, numerous schemes have been proposed. [11] designed a Diffie-Hellman-MAC key exchange system that functions efficiently using the keyed MAC hash function. [12] created a redesigned internet architecture that decreased the likelihood of covert network attacks. They strengthened the security of the encryption protocol by enhancing the existing algorithm with additional security codes. [13] developed an advancement in the Diffie-Hellman Algorithm. They applied certain mathematical algorithms to make the communication secure. [14] developed a version of the Diffie-Hellman key exchange that secures communication networks by utilizing the Blowfish encryption method.

Algorithm of the Diffie-Hellman Key Exchange

The algorithm of the Diffie-Hellman key exchangestates sequentially the step-by-step procedures to generating the common secret key in a cryptographic system.
The steps include;

(1) Both parties agree on p and q, two positive numbers, where q is a group generator and p is a positive prime number.
(2) Both parties randomly choose their private keys, say x and y respectively
(3) Both parties calculate their public keys
$K_a = q^x \bmod p$ and $K_b = q^y \bmod p$
(4) Both parties exchange their public keys to compute the common shared key
$K_{ab} = q^{xy} \bmod p$

3. CONCEPTUAL FRAMEWORK OF THE NEW SYSTEM

Figure 3 illustrates the conceptual framework of the Diffie-Hellman key exchange method. It consists of two parties, each with their own private and public key. While the public key is shared by all participants in the communication system, the private keys are kept confidential.

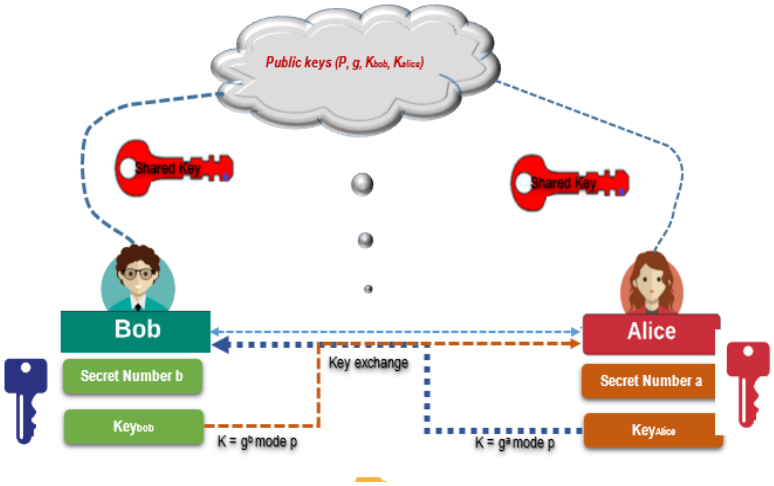

Figure 3: Conceptual design of the Diffie-Hellman Key Exchange Algorithm

4. OBJECT-ORIENTED DESIGN PROCESS MODEL

[15] described the software engineering method known as the Object-Oriented Analysis and Design (OOAD) model, which shows an architecture as a collection of interrelated entities working together to address a specific problem.

Each entity in the object-oriented paradigm represents a set of real-world entities connected by methods and properties. Classes including data and methods are developed in object-oriented models, along with the methods needed to manipulate the data. Unified Modeling Language designs for object-oriented model picture system.

The Unified Modeling Language is a graphical language utilised to define, construct, picture, and document software system components. The use-case, class, sequence, and activity diagrams are among the artifacts that the researchers employed in the present paper.

5. ANALYSIS OF THE DIFFIE-HELLMAN ALGORITHM USING A USE-CASE DIAGRAM

5.1. Use-Case Diagram of the Diffie-Hellman Algorithm

The use case diagram shows a system's functionality from the perspective of an outside observer [16]. It is a systematic method of acquiring data regarding the needs of a system as seen by its users. Use cases, relationships, and actors make up its three main parts. To accomplish the user's goal, an actor interacts with the system's use cases. Figure 4 shows the use-case diagram of the Diffie-Hellman key exchange algorithm.

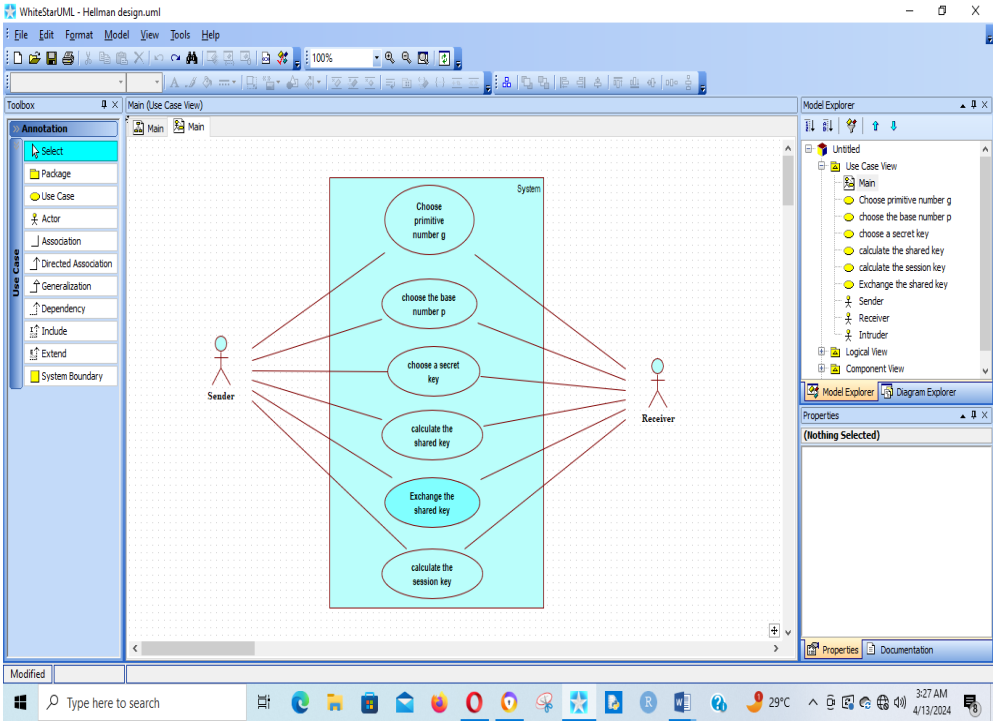

Figure 4: Use-case diagram of the Diffie-Hellman Key Exchange

5.2. Diffie-Hellman Key Exchange Activity Diagram

An activity diagram represents the way controls are transferred from one task to another. It shows a series of operations that are performed on part of classes in the system. Figure 5 shows the activity diagram of the Diffie-Hellman key exchange algorithm.

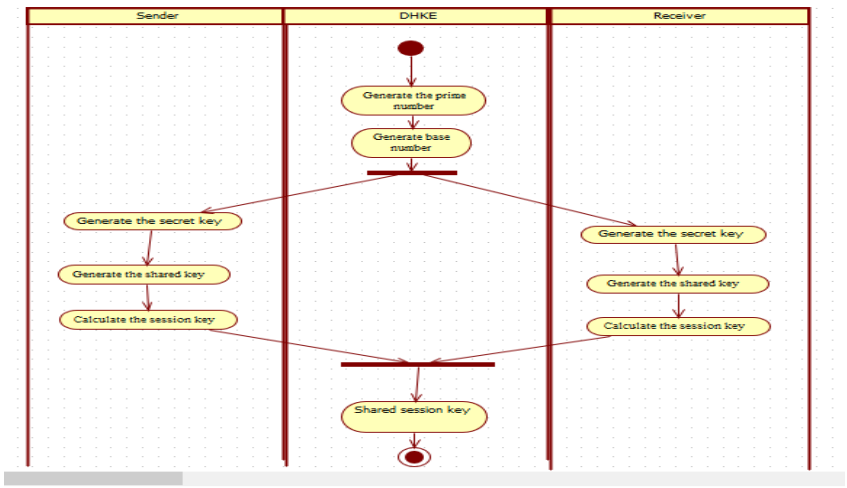

Figure 5: Activity diagram of the Diffie-Hellman key exchange

5.3. Sequence Diagram of the Diffie-Hellman Key Exchange

A sequence diagram is a diagram that shows the interactions between different objects in a sequential order. It represents the flow of messages from one object to another. The main

objective of a sequence diagram is to represent how messages are exchanged between objects. Figure 6 displays the Diffie-Hellman key exchange cryptosystem's sequence diagram.

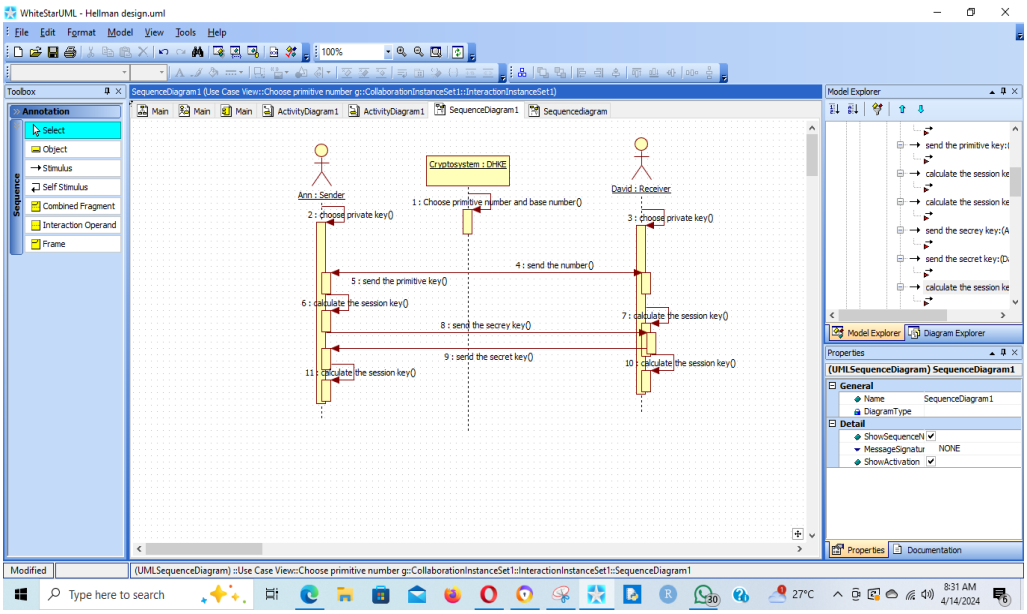

Figure 6: Sequence diagram of the proposed cryptosystem

6. DIFFIE-HELLMAN KEY EXCHANGE DESIGN USING CLASS DIAGRAM

A class diagram is a rigid framework that illustrates the classes, properties, methods, and interactions between the classes in a cryptosystem to describe its framework. Class names, attributes, and methods are the three sections that make up a class in class diagrams. Class diagrams also use concepts like inheritance, association, multiplicity, and visibility. The class diagram for the proposed Diffie-Hellman key exchange algorithm is depicted in Figure 7.

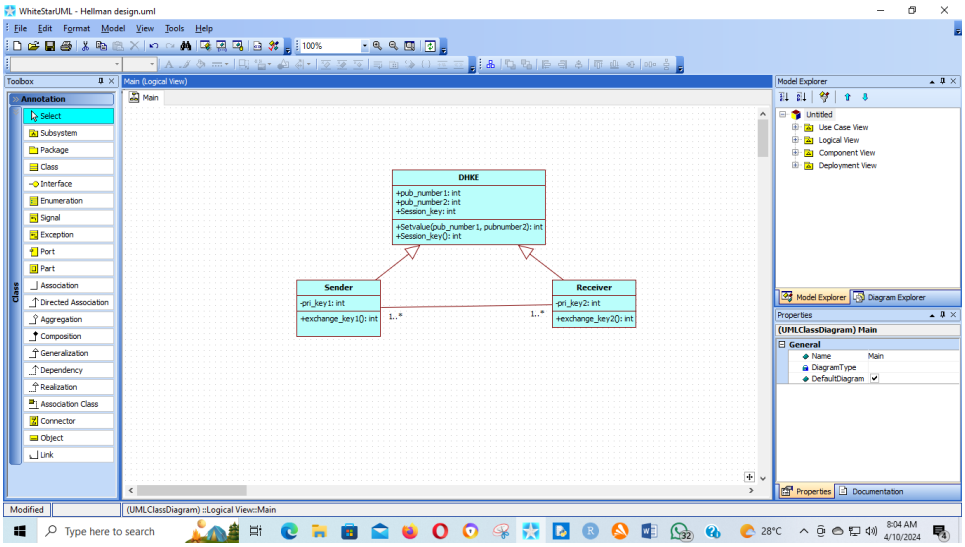

Figure 7: Diffie-Hellman key exchange class diagram

The class diagram, in Figure 8, has three classes (DHKE), sender and receiver. Both transmitter and receiver classes in the class diagram are offspring of the parent class (DHKE), and they acquire the methods and properties of their parent class (DHKE).

7. IMPLEMENTATION

Object-oriented programming languages have implemented the Diffie Hellman key exchange algorithm. The programming language C++ was employed in this work. The researchers put the three classes to the test during the implementation phase. Sender, Receiver, and Cryptosystem constitute the classes. As the offspring of the cryptosystem (DHKE), the sender and recipient acquire the attributes and functions of the cryptosystem. They implemented the Diffie Hellman key exchange algorithm using C++ object-oriented programming language.

8. CONCLUSION

The study has demonstrated that object-oriented modeling techniques can be used to explain the Diffie-Hellman key exchange algorithm. The modeling technique enabled communicating parties in a cryptosystem to act like real-world things with encapsulated attributes and methods.

ACKNOWLEDGMENT

We would like to express our gratitude to our friends and families for their moral and financial assistance in getting this work published.

REFERENCES

[1] Ashioba, N. C and Yoro, R. “RSA Cryptosystem using Object-Oriented Modeling Technique,” International Journal of Information and Communication Technology Research, vol. 4, no. 2, pp. 57-61, 2014.

[2] DharitriTalukdar, Prof (Dr.) Lakshmi P. Saikia. A Review On Different Encryption Techniques: A Comparative Study. International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015 ISSN 2091-2730

[3] Forouzan B. A. “Data Communication and Networking (4 Edition)”, McGraw Hill Inc. New York, 2008.

[4] Kaushik A. and Satvika, “Extended Diffie-Hellman Algorithm for key Exchange and Management” International Journal of Advances in Engineering Sciences. Vol. 3(3) pp. 67-70, July 2013.

[5] SharadBoni, JaimikBhayy, and Santosh Bhat. Improving the Diffie-Hellman key exchange Algorithm by proposing the multiplicative key exchange Algorithm. International Journal of Computer Application Vol. 130, No. 15, 2015.

[6] Chavan, A., Jadhav, A., Kumbhar, S. and Joshi, I. Data Transmission using RSA Algorithm. International Research Journal of Engineering and Technology (IRJET) Vol. 6 Issue 3, Mar. 2019.

[7] Abari, O. J., Shola, P. B. and Philip S.Comparative Analysis of Discrete Logarithm and RSA Algorithm in Data Cryptography. International Journal of Computer Science and Information Security, Vol. 13, No. 2 2015.

[8] Navpreet K., and Nagpal R. Authenticated Diffie-Hellman Key Exchange Algorithm. International Journal of Computer Science and Information Technologies Vol. 5 Issue 4., 2014

[9] Subrahmanyeswara Rao S. V. B, and Yalamanchili. Anjani. An Approach to Public-Key Cryptography using Diffie - Hellman Key Exchange Algorithm. International Journal for Research in Engineering Application & Management (IJREAM) ISSN: 2454-9150 Vol-03, Issue-08, Nov 2017

[10] Emmanuel Bresson, Olivier Chevassut,David Pointcheva, and Jeanuser A wish to set u a connection with user B and use a Jacques Quisquater, "Authenticated Group Diffie-Hellman Key Exchange",

Computer and Communication Security- proc of ACM CSS'OI, Philadelphia, Pennsylvania, USA, Pages 255-264, ACM Press, November 5-8, 2001.

[11] Eun-Jun Yoon and Kee-Young Yoo, "An Efficient Diffie- HellmanMAC Key Exchange Scheme", 2009 Fourth International Conference on Innovative Computing, Information, and Control.

[12] Vinothini, Sarany, Vasumathl A Study on Diffie-Hellman Algorithm in Network Security. International Journal of Engineering and Computer Science ISSN:2319-7242 volume 3 Issue 7 July 2014 Page No. 7346-7349

[13] MonalisaJha and Shraddha Patil (2015). Advancement in Diffie-Hellman Algorithm. ManolisaJha' Int Journal of Engineering Research and Applications. ISSN -2248-9622. Vol 5, Issue 7 July 2015, pp1-2.

[14] Aldo Adrian, Maya Cendana, SilvereDiah Handy Permana. Diffie-Hellman Key Exchange Modification using Blowfish Algorithm to prevent logjam attack. Journal of Telecommunication, Electronic and Computer Engineering ISSN 2180-1843. Vol 10, No 4; 2018.

[15] Dhiman, K. S., Shatma, A., and Kaur A. "Comprehensive Study of Object Oriented Anaylsis and Design by using the Concept of OOSE"International Journal of Research in Education Methodology Vol. 1, No. 1. pp. 14-16, 2012.

[16] Nayak R., Patheja P. S., and Waoo A. A. "Design of Weather Forecasting System through unified modeling language". International Journal of Research in Engineering and Applied Sciences Vol. 2 (2) pp. 1189-1194, 2012.