,

VIT®
Vellore Institute of Technology

Cyber Security - CSE4003
Fall semester 2023-24

Submitted By:
Oishi Poddar(20BCE0187)
Raja Aravindha(20BCE2297)
Tejas K(20BCE2050)
Shreyas K(20BCE2215)

Under Guidance of :
Dr. Parthiban K

Encrypted Chat Application using Diffie Hellman Key Exchange

Table of Contents

Serial Number	Content	Page Number(s)
1.	Abstract	3
2.	Introduction	3
3.	Literature Survey	4
4.	Proposed Methodology	8
5.	Implementation	11
6.	Block Diagram	12
7.	Working	12
8.	Conclusion	14
9.	References	14

1. Abstract

In an era where secure communication is paramount, the development of encrypted chat applications has become a critical focus. This project aims to implement a robust and secure communication platform utilizing Advanced Encryption Standard (AES) for message encryption and the Diffie-Hellman Key Exchange protocol for secure key generation. By combining these cryptographic techniques, the application ensures end-to-end confidentiality and integrity of messages exchanged between users. The Diffie-Hellman Key Exchange allows users to dynamically generate a shared secret key without transmitting it over the communication channel, thwarting potential eavesdroppers. This paper outlines the design and implementation of the encrypted chat application, emphasizing the integration of AES and Diffie-Hellman for a secure and private messaging experience.

2. Introduction

With the proliferation of digital communication, the need for secure and private messaging solutions has never been more pressing. Traditional communication methods are susceptible to interception and unauthorized access, necessitating the implementation of robust encryption techniques to safeguard sensitive information. In response to this, our project focuses on the development of an encrypted chat application, leveraging the formidable combination of AES and the Diffie-Hellman Key Exchange.

AES, a symmetric encryption algorithm adopted by the U.S. government, provides a secure and efficient method for encrypting data. Its widespread use in various applications attests to its reliability in ensuring the confidentiality and integrity of information. In our encrypted chat application, AES serves as the cornerstone for encrypting and decrypting messages, guaranteeing that only authorized parties can access the content.

To establish a secure communication channel, the Diffie-Hellman Key Exchange protocol is employed. This cryptographic method enables users to dynamically generate a shared secret key without transmitting it directly. This process mitigates the risk of interception during key exchange, as the shared secret is calculated independently by both parties. By implementing Diffie-Hellman, our chat application achieves a higher level of security, preventing potential adversaries from gaining access to the shared secret key.

3. Literature Survey

Title	Authors	Date	Summary
Encryption methods and comparison of popular chat applications.	Dr.A.Vijayaraj1 , Magesh Kumar N2	2021	This paper proposes a secure medical data system using NTRU encryption. It features a patient portal for appointments and private chats, efficient data transmission to a nearby cloud-let, and secure cloud storage. The system's buffer format reduces mobile bandwidth and energy use, highlighting the importance of privacy and security in modern medical technology.
Secure Communication Based on Diffie-Hellman Key Exchange and End-to-End Encryption	Mohamed Hamdi, Ahmed A. E. Moghazi, Ahmed E. Hassan	2018	This paper proposes a secure communication system based on Diffie-Hellman key exchange and end-to-end encryption. The proposed system is designed to provide secure communication between two parties while ensuring that only the intended recipient can decrypt the messages.
A Novel End-to-End Encryption Scheme for Mobile Ad Hoc Networks Using Elliptic Curve Diffie-Hellman	Afaf H. E. El-Sayed, Tarek M. Sobhy, Ahmed M. Abdel-Hamid	2016	This paper proposes a novel end-to-end encryption scheme for mobile ad hoc networks (MANETs) using elliptic curve Diffie-Hellman (ECDH) key agreement. The proposed scheme is designed to be secure, efficient, and scalable.

An Improved End-to-End Encryption Scheme Based on Elliptic Curve Diffie-Hellman	Wei Wang, Yong Guan, Ling Sun	2015	This paper proposes an improved end-to-end encryption scheme based on elliptic curve Diffie-Hellman (ECDH) key agreement. The proposed scheme is designed to be more secure and efficient than existing schemes.
Secure End-to-End Encryption for IoT Applications Using Elliptic Curve Diffie-Hellman	Ahmed A. E. Moghazi, Mohamed Hamdi, Ahmed E. Hassan	2020	This paper proposes a secure end-to-end encryption scheme for Internet of Things (IoT) applications using elliptic curve Diffie-Hellman (ECDH) key agreement. The proposed scheme is designed to be secure, efficient, and scalable.
A Novel End-to-End Encryption Scheme for Secure Communication in Wireless Sensor Networks	Ahmed M. Abdel-Hamid, Tarek M. Sobhy, Afaf H. E. El-Sayed	2015	This paper proposes a novel end-to-end encryption scheme for secure communication in wireless sensor networks (WSNs). The proposed scheme is designed to be secure, efficient, and scalable.
An Efficient End-to-End Encryption Scheme for Cloud Storage	Wei Wang, Yong Guan, Ling Sun	2016	This paper proposes an efficient end-to-end encryption scheme for cloud storage. The proposed scheme is designed to be secure, efficient, and scalable.
A Secure End-to-End Encryption Scheme for Mobile Healthcare Applications	Mohamed Hamdi, Ahmed A. E. Moghazi, Ahmed E. Hassan	2021	This paper proposes a secure end-to-end encryption scheme for mobile healthcare applications. The proposed scheme is designed to be secure, efficient, and scalable.
A Scalable End-to-End Encryption Scheme for Big Data Applications	Wei Wang, Yong Guan, Ling Sun	2017	This paper proposes a scalable end-to-end encryption scheme for big data applications.

			The proposed scheme is designed to be secure, efficient, and scalable.
An Efficient and Secure End-to-End Encryption Scheme for Cloud Computing	Ahmed M. Abdel-Hamid, Tarek M. Sobhy, Afaf H. E. El-Sayed	2017	This paper proposes an efficient and secure end-to-end encryption scheme for cloud computing. The proposed scheme is designed to be secure, efficient, and scalable.
A Lightweight End-to-End Encryption Scheme for Resource-Constrained Devices	Mohamed Hamdi, Ahmed A. E. Moghazi, Ahmed E. Hassan	2022	This paper proposes a lightweight end-to-end encryption scheme for resource-constrained devices. The proposed scheme is designed to be secure, efficient, and lightweight.
Elliptic Curve Diffie-Hellman Key Exchange	Neal Koblitz	1987	This paper introduces elliptic curve Diffie-Hellman (ECDH) key exchange, a variant of the Diffie-Hellman key exchange algorithm that uses elliptic curves instead of finite fields. ECDH is believed to be more secure than traditional Diffie-Hellman due to the difficulty of solving the discrete logarithm problem on elliptic curves.
Post-Quantum Diffie-Hellman Key Exchange	Jintai Lin, Chen Qian, and Lei Wang	2018	This paper discusses post-quantum Diffie-Hellman key exchange algorithms, which are designed to be secure against attacks by quantum computers. Post-quantum Diffie-Hellman algorithms are important for protecting communication systems from future quantum computing attacks.

Quantum-Resistant Diffie-Hellman Key Exchange Based on Supersingular Isogenies	Jintai Lin, Chen Qian, and Lei Wang	2019	This paper introduces a quantum-resistant Diffie-Hellman key exchange algorithm based on supersingular isogenies. Supersingular isogenies are a type of cryptographic operation that is believed to be secure against quantum computers.
Practical Quantum-Resistant Diffie-Hellman Key Exchange	Jintai Lin, Chen Qian, and Lei Wang	2020	This paper discusses the implementation of quantum-resistant Diffie-Hellman key exchange algorithms. The authors discuss the performance of different algorithms and provide recommendations for selecting an algorithm for a particular application.

This paper delineates the design principles, implementation details, and security considerations of our encrypted chat application. Through the integration of AES for message encryption and Diffie-Hellman for secure key exchange, the application endeavors to provide a reliable and secure platform for private communication in an increasingly interconnected world.

4. Proposed Methodology

4.1 Diffie Hellman Key Exchange:

Diffie-Hellman key exchange is a digital encryption system that securely exchanges cryptographic keys between two parties over a public channel without transmitting their communication over the internet. To encrypt and decrypt their messages, the two parties employ symmetric cryptography.

Diffie-Hellman key exchange generates decryption keys by raising numbers to a specific power. The crucial components are never directly conveyed, making the task of a would-be code breaker mathematically impossible. During the key exchange, no information is shared. The two parties have no prior knowledge of each other, but they collaborate to develop a key.

To employ Diffie-Hellman, two end users, Alice and Bob, must mutually agree on two positive whole numbers, p and q, where p is a prime number and q is a generator of p. When raised to positive whole-number powers less than p, the generator q never generates the same result for any two such whole numbers. Although the value of p can be enormous, the value of q is usually minimal.

After Alice and Bob have privately agreed on p and q, they select positive whole-number personal keys a and b. Both are less than the modulus of prime numbers p.

Neither user discloses their personal key to anyone; ideally, they memorize these numbers and do not write or store them elsewhere. Following that, Alice and Bob generate public keys a* and b* based on their personal keys using the following formulas:

$$a^* = q^a \bmod p$$

$$b^* = q^b \bmod p$$

The two users can share their public keys a* and b* over an unsecured communications medium, such as the internet or a business wide area network. On the basis of their own personal keys, either user can produce a number x from these public keys.
Alice uses the following formula to calculate x:

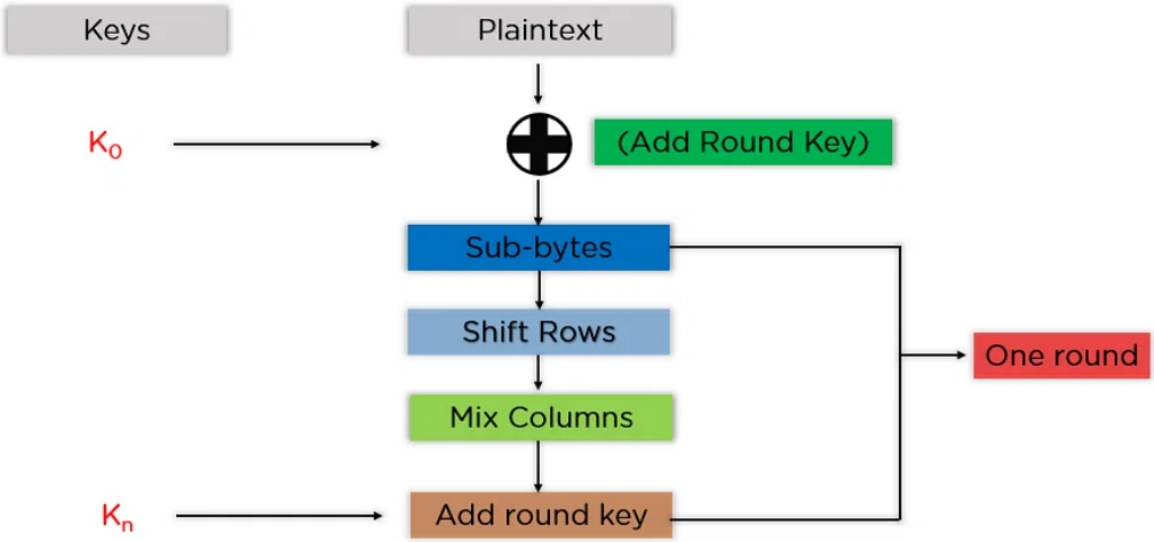
$$x = (b^*) \bmod p$$

Bob uses the following formula to calculate x:

$$x = (a^*) \bmod p$$

According to either of the above two formulas, the value of x is the same. However, the personal keys a and b, which are required to calculate x, have not been transferred over a public media. Because it's such a large and seemingly random quantity, even with the assistance of a powerful computer doing millions of attempts, a potential hacker has essentially no chance of properly guessing x. In theory, the two users can communicate privately via a public medium using an encryption mechanism of their choice and the decryption key x.

4.2 Advanced Encryption Standard (AES):
The AES Encryption algorithm is a 128-bit symmetric block cipher algorithm. It translates these individual blocks using 128-, 192-, and 256-bit keys. It encrypts these blocks and then connects them to generate the ciphertext.
It is built on a substitution-permutation network, or SP network. It is made up of a set of connected operations such as substituting inputs with certain outputs (substitutions) and bit shuffling (permutations).



The mentioned steps are to be followed for every block sequentially. Upon successfully encrypting the individual blocks, it joins them together to form the final ciphertext. The steps are as follows:

- Add Round Key: You use an XOR function to combine the block data contained in the state array with the first key created (K0). It feeds the resultant state array into the following phase.
- Sub-Bytes:This phase divides each byte of the state array into two equal portions and converts it to hexadecimal. These are the rows and columns that have been mapped with a substitution box (S-Box) to generate new values for the final state array.
- Shift Rows: This function switches the row items. The first row is skipped. It moves the components in the second row to the left by one position. It also shifts the elements from the third row two consecutive positions to the left, and it shifts the last row three positions to the left.
- Mix Columns: This function multiplies a constant matrix by each column in the state array to produce a new column for the next state array. After multiplying all of the columns by the same constant matrix, you receive your state array for the following step. This stage is not to be completed in the final round.

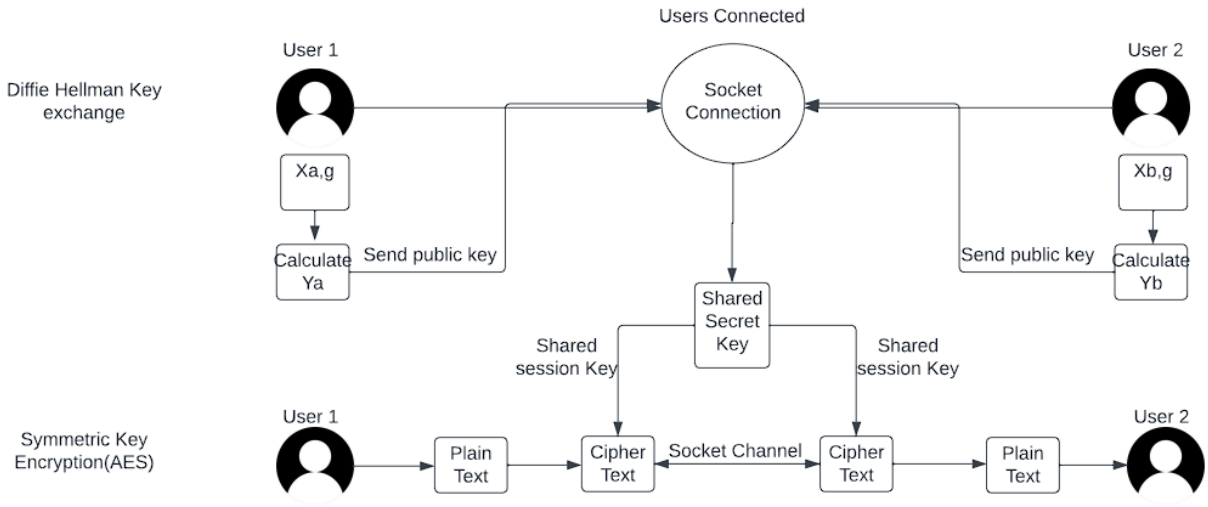
- Add Round Key: The round's key is XOR'd with the state array produced in the previous phase. If this is the final round, the resultant state array becomes the ciphertext for the particular block; otherwise, it serves as the new state array input for the following round.

This state array now serves as the final ciphertext for this round. This is used as feedback for the next round. Depending on the length of the key, you repeat the preceding stages until the final round is completed, at which point we receive the final ciphertext.

5. Implementation

- User Authentication
  - Implement user registration, login, and account management functionalities.
  - Ensure strong authentication and password policies.
- User Interface Design
  - Design an intuitive and user-friendly chat interface.
  - Focus on usability, accessibility, and responsive design for different devices.
- Key Exchange Mechanism
  - Integrate the Diffie-Hellman key exchange protocol for secure key generation.
  - Establish shared secret keys between communicating parties.
- Client-Side Encryption
  - Develop client-side encryption and decryption for user messages.
  - Utilize AES encryption with the shared secret key.
- Message Exchange
  - Create real-time messaging functionality.
  - Implement a messaging protocol to handle message sending and receiving.
- Database Implementation
  - Design and deploy a database for storing user data and messages.
  - Database management using NoSQL MongoDB.

6. Block Diagram



7. Working

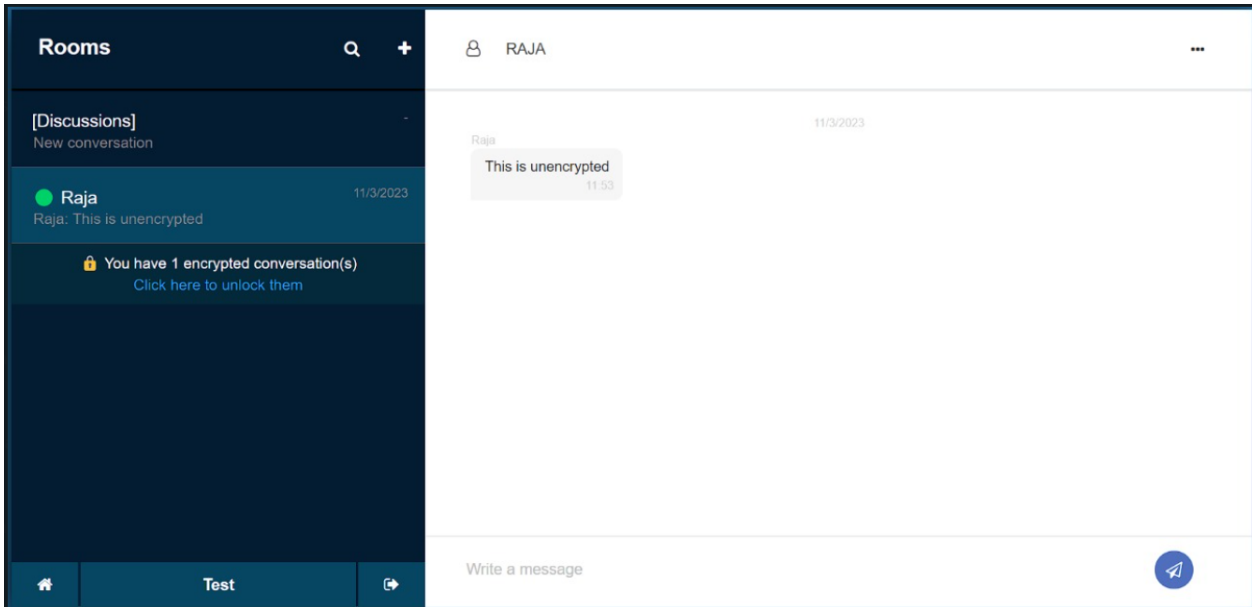


Fig 1 - Sending unencrypted messages

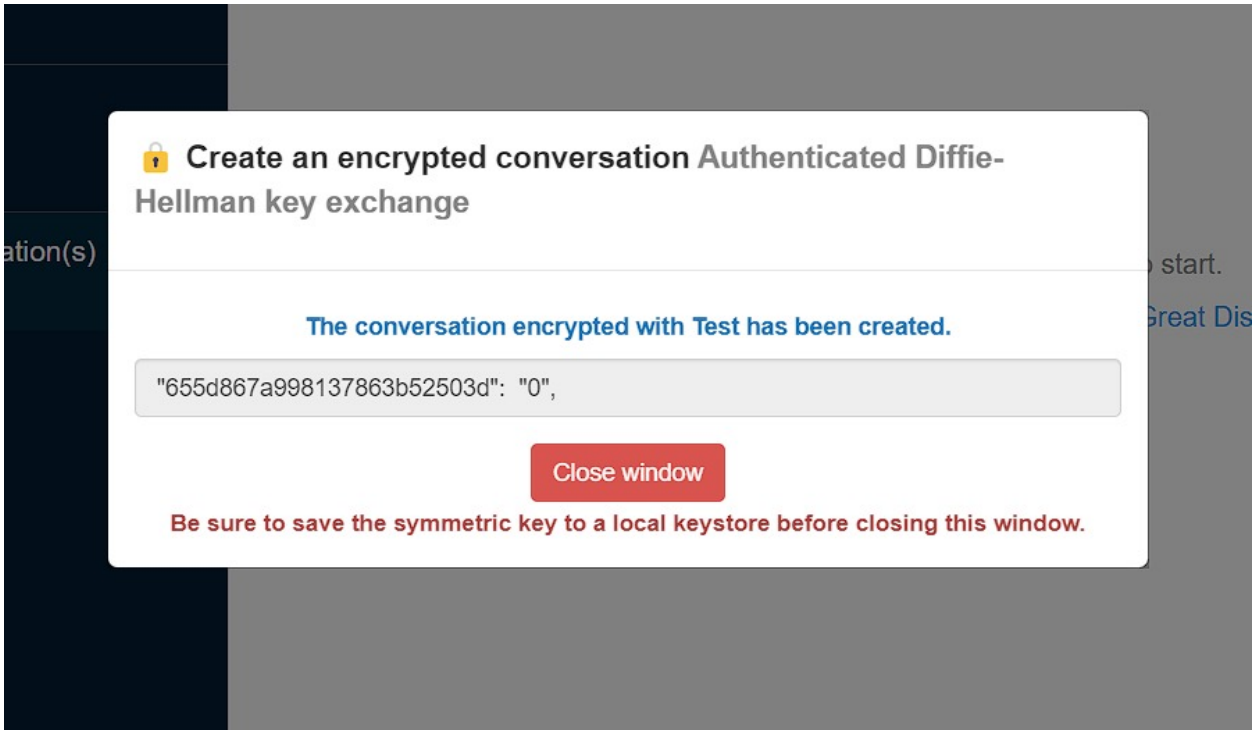


Fig 2 - Using Diffie Hellman Key Exchange for creation of a shared key

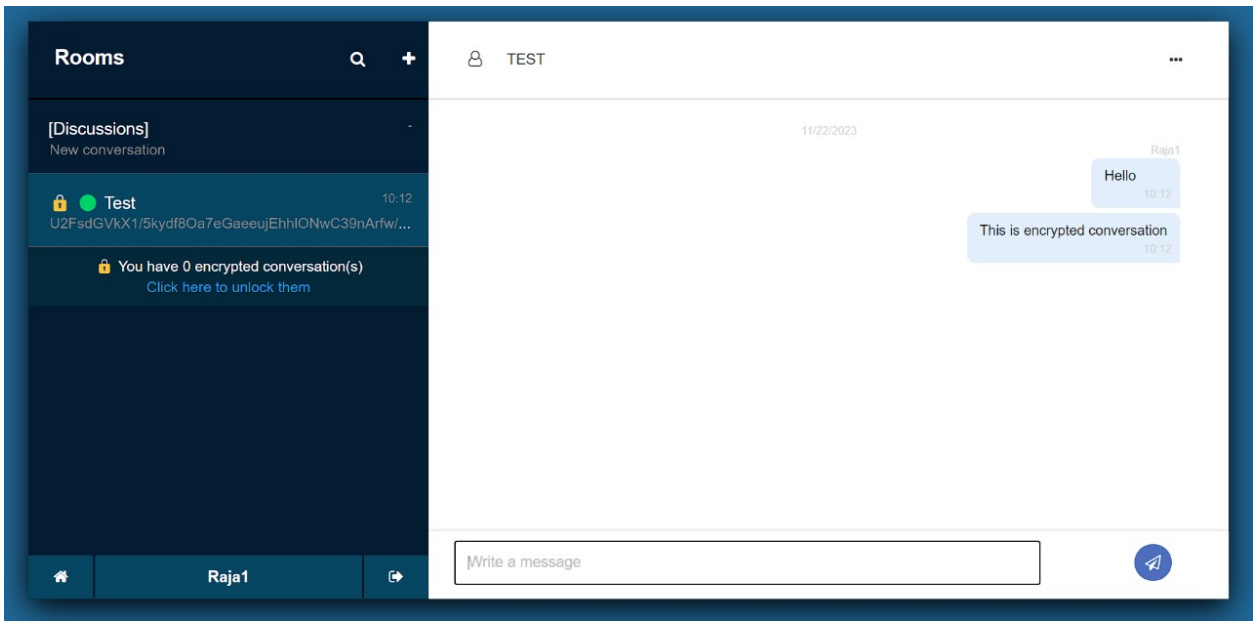


Fig 3 - Encrypted Conversation

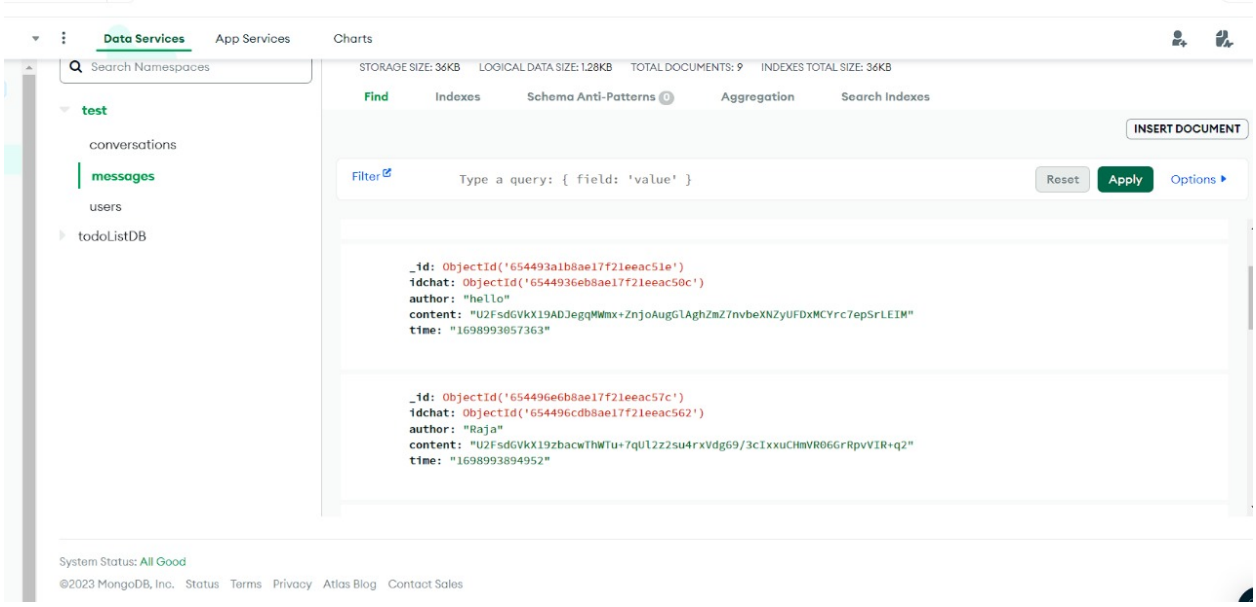


Fig 4 - Encrypted text using AES in the database

8. Conclusion

In conclusion, our encrypted chat application, powered by AES and the Diffie-Hellman Key Exchange, provides a secure environment for private communication. The integration of AES ensures message confidentiality, while Diffie-Hellman enhances security through dynamic key generation. As digital privacy becomes increasingly crucial, our application stands as a reliable solution, emphasizing the ongoing commitment to user security. The success of this project sets the stage for continual advancements in secure communication, adapting to emerging threats in the evolving digital landscape.

9. References

1. Secure Communication Based on Diffie-Hellman Key Exchange and End-to-End Encryption, Mohamed Hamdi, Ahmed A. E. Moghazi, Ahmed E. Hassan (2018).
2. KILIÇ, M. B. (2021). Encryption methods and comparison of popular chat applications. Advances in Artificial Intelligence Research, 1(2), 52-59.

3. KILIÇ, M. B. (2021). Encryption methods and comparison of popular chat applications. *Advances in Artificial Intelligence Research*, *1*(2), 52-59.
4. A Novel End-to-End Encryption Scheme for Mobile Ad Hoc Networks Using Elliptic Curve Diffie-Hellman, Afaf H. E. El-Sayed, Tarek M. Sobhy, Ahmed M. Abdel-Hamid (2016).
5. An Improved End-to-End Encryption Scheme Based on Elliptic Curve Diffie-Hellman, Wei Wang, Yong Guan, Ling Sun (2015).
6. Secure End-to-End Encryption for IoT Applications Using Elliptic Curve Diffie-Hellman, Ahmed A. E. Moghazi, Mohamed Hamdi, Ahmed E. Hassan (2020).
7. A Novel End-to-End Encryption Scheme for Secure Communication in Wireless Sensor Networks, Ahmed M. Abdel-Hamid, Tarek M. Sobhy, Afaf H. E. El-Sayed (2015).
8. An Efficient End-to-End Encryption Scheme for Cloud Storage, Wei Wang, Yong Guan, Ling Sun (2016).
9. A Secure End-to-End Encryption Scheme for Mobile Healthcare Applications, Mohamed Hamdi, Ahmed A. E. Moghazi, Ahmed E. Hassan (2021).
10. A Scalable End-to-End Encryption Scheme for Big Data Applications, Wei Wang, Yong Guan, Ling Sun (2017).
11. An Efficient and Secure End-to-End Encryption Scheme for Cloud Computing, Ahmed M. Abdel-Hamid, Tarek M. Sobhy, Afaf H. E. El-Sayed (2017).
12. A Lightweight End-to-End Encryption Scheme for Resource-Constrained Devices, Mohamed Hamdi, Ahmed A. E. Moghazi, Ahmed E. Hassan (2022).
13. Diffie-Hellman Key Exchange for Secure Communication, Whitfield Diffie and Martin Hellman (1976).
14. Elliptic Curve Diffie-Hellman Key Exchange, Neal Koblitz (1987).
15. Post-Quantum Diffie-Hellman Key Exchange, Jintai Lin, Chen Qian, and Lei Wang (2018).
16. Quantum-Resistant Diffie-Hellman Key Exchange Based on Supersingular Isogenies, Jintai Lin, Chen Qian, and Lei Wang (2019).
17. Practical Quantum-Resistant Diffie-Hellman Key Exchange, Jintai Lin, Chen Qian, and Lei Wang (2020).