College of computers & Artificial intelligence technology CAIT

Misr University for Science & Technology (MUST)
College of Information Technology
Department of Computer Science

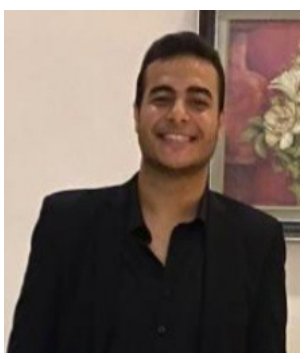
Under the Supervision of

Prof. Dr. Rania Elgohary

Eng.Nehal A. Mohamed

Eng.Islam Saied

Team


Fouad Mostafa
89638


Abdelrahman Fathy
89393

Wannahide


Abdallah Riad
89683


Mahmoud Mohammed
89401

Abstract

Digital communication is essential globally, but securing data is challenging. Encryption algorithms are necessary as they ensure confidentiality of the data.In WANNA-HIDE a hybrid encryption scheme based on Elgamal algorithm and AES-256-CBC along with double ratchet protocol is used, to provide end-to-end encryption which guarantees a secure channel for communication between parties

Introduction

The increasing frequency and severity of data breaches in recent years have highlighted the critical importance of security and privacy in today's digital world. From financial institutions to social media platforms, no organization is immune to the risk of data breaches, which can lead to significant financial losses and reputation damage.

Methodology

WannaHide is a secure chatting app that uses hybrid encryption scheme which involves two algorithms, Elgamal algorithm as an asymmetric encryption to ensure a secure key exchange process between parties, and AES-256-CBC representing the symmetric encryption algo-rithm which is responsible for encrypting the actual data sent between the users. In addition double ratchet protocol is implemented to provide more security.

Results

Encryption/Decryption processes for plain text data and images are done with no flaws and delivered the desired results, Elgamal algorthim has proven to be more secure and chellenging to solve than RSA even though RSA is faster in encryption process only, and Elgamal is better in terms of memory consumption for both encryption and decryption

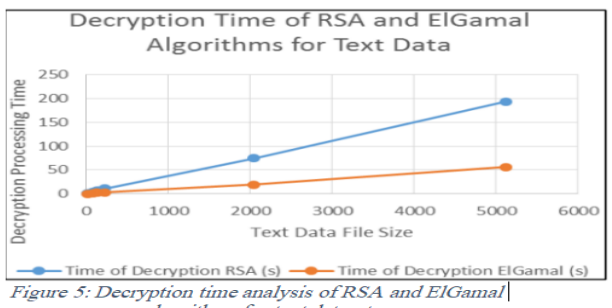


Figure 5: Decryption time analysis of RSA and ElGamal algorithms for text dataset

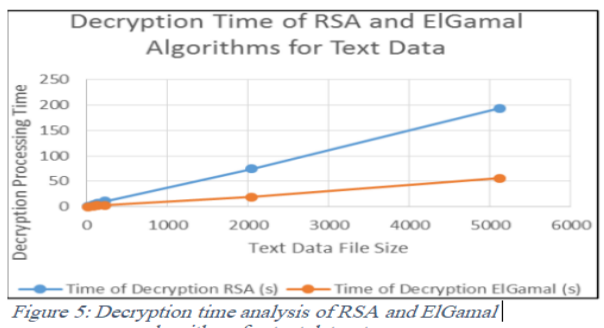


Figure 5: Decryption time analysis of RSA and ElGamal algorithms for text dataset

Future work

In our next phase, we expect that our website will be launced as soon as possible , we will finish the implementation, and the website will be ready for use and serve the people along with expanding application functionalities to support video and file encryption, in addition, providing vioce over ip calls .

Conclusion

Purpose of Wannahide is to make instant messaging service more secure through double ratchet end-to-end encryption based on an enhanced algorithm of Diffie-hellman called Elgamal algorithm that made encryp-tion process more secure, faster and less vulnerable to practical attacks that threats the confidentiality of the communication process.

Refrences

[1]Mallouli, F., Hellal, A., Saeed, N. S., & Alzahrani, F. A. (2021, June). A survey on cryptography: comparative study between RSA vs ECC
[2]algorithms, and RSA vs El-Gamal algorithms. In 2019 6th IEEE ,International Conference on Cyber Security and Cloud Computing
[3] Kurnia, H. Dafitri, and A. P. U. Siahaan, "RSA 32-bit Implementation Technique," Int. J. Recent Trends Eng. Res., vol. 3, no. 7, pp. 279–284, 2017