

CNS PROJECT REPORT

End to End Encryption in Chat Application

SEMESTER : 5th SEMESTER

BRANCH : INFORMATION TECHNOLOGY

BATCH : B-11

GROUP NO. : 7

FACULTY NAME : MS. KAVITA PANDEY

COURSE CODE : 18B11CS212

STUDENT DETAILS: AMIT G. PATIL - 19104004





SANJOLI GOYAL - 19104007

MUSKAN JAIN - 19104010

MANU SINGH BIST - 19104041

Declaration

We hereby declare that this submission is our own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text. We accept the use of the material presented in this report for Education/Research/Teaching purpose by the faculty.

			
Amit Patil	Sanjoli Goyal	Muskan Jain	Manu Singh Bist
11 Nov 2021 Mumbai	11 Nov 2021 Hathras	11 Nov 2021 Meerut	1 Nov 2021 Noida

Abstract

In the era of active digital communication we are experiencing data breaches and security problems compromising our privacy and having Identity theft. This problem is accelerating day by day and increasing exponentially. Many data (photographs, messages) that should be kept confidential based on individual or society have become the limits with the developing technology. The purpose of the report is to propose end-to-end encryption provided chat applications where user individuals can exchange private information securely and rely on scaleable, secure E2EE algorithm.

Table of Content

[Declaration](#)

[Abstract](#)

[Table of Content](#)

[Introduction](#)

[Literature Review](#)

[Different Encryption Algorithms Used in Messaging Platforms](#)

[1. DES](#)

[2. 3DES](#)

[3. AES](#)

[4. Diffie Hellman Key Exchange \(DHKE\)](#)

[5. RSA](#)

[Gaps in Research Papers](#)

[Research Papers](#)

Introduction

End-to-end encryption (E2EE) is the best-known way to protect users' digital communications, as it prevents service providers as well as unassociated third parties from reading messages. In recent years, several popular messaging apps have adopted end-to-end encryption, either by default (WhatsApp, iMessage) or as an optional feature (Facebook Messenger, Telegram). As a result, after decades of use only in niche applications and communities, E2EE is now readily available and used by millions or even billions of users.

Literature Review

Encryption is widely used in applications and communications to ensure information confidentiality. Several group chat applications benefit from the use of some type of mechanism that guarantees the confidentiality of information. Some of the most used message exchange applications were chosen to identify and evaluate the characteristics and encryption mechanisms of these applications, to identify the most suitable ones to be used in the development of the application proposed in this paper.

Messaging Applications-

1. **Signal.** Signal is one of the most used protocols due to its encryption techniques and open-source code. The Signal protocol stood out due to the following applied techniques:
 - a. **KDF (Key Derivation Functions)**
 - b. **Double ratchet algorithm**
 - c. **AES256**
 2. **Whatsapp.** WhatsApp is a closed source instant messaging protocol. The WhatsApp stood out due to the following applied techniques:
 - a. **The Signal key exchange protocol, consisting of the X3DH Key Agreement Protocol**
 - b. **Double ratchet algorithm**
 3. **Telegram.** Telegram, which offers an open-source messaging service, uses its own cryptographic encryption protocol, MTProto. Encryption operations are based on
 - a. **256-bit symmetric AES encryption,**
 - b. **2048-bit RSA encryption,**
 - c. **Diffie-Hellman key exchange.**
 4. **Viber.** UNH Cyber Forensics research revealed explicitly that Viber is not secure at all in many cases. The research has revealed that media files such as pictures
-

or videos which are transferred between the users have no encryption and the data is stored on the Viber server unencrypted, with no end to end encryption.

- a. **Concept of “Double Ratchet”**
 - b. **128-bit Symmetric Key**
 - c. **Asymmetric ECC**
5. **Facebook Messenger.** Facebook Messenger is a popular messaging service available for Android and iOS. It provides two messaging modes for normal chat and private chat. Standard chat uses only TLS, does not provide end-to-end encryption, and stores all messages on its servers. Private Chat uses the following techniques.
 - a. **Signal Protocol to provide end-to-end encryption between sender and recipient.**

Different Encryption Algorithms Used in Messaging Platforms

1. DES

- First Encryption Standard
- Block Cipher with 64 bit block size
- 64 bit key length
- However it was proved to be insecure

2. 3DES

- Improved DES
- Block Size= 64 bit
- 192 bit key size
- Encryption method used in DES applied 3 times
- Increased encryption level and average safe time
- However it was slower than any block cipher

3. AES

- Block cipher
 - Variable key length of **128, 192 or 256** bits
 - Block size= 128 bits
 - Fast and flexible
 - Can be used on various platforms
 - However it uses symmetric key algorithm, same keys are potentially vulnerable to attacks
-

4. Diffie Hellman Key Exchange (DHKE)

- Symmetric cryptography technique
- Highly secure
- However it posed two problems for the users
 1. The users of the algorithm need to share the private key to encrypt or decrypt the data; this was achieved by either physically meeting the person before sending data, or sending the keys via a network. Both ways were pretty inefficient.
 2. The other problem was the sender or the receiver had to keep track of all the keys of different receiver or sender respectively which was a headache for users who communicate with large groups like a corporate.

5. RSA

- Variable size encryption block
- Variable size key
- High security
- 2 Prime numbers used to generate
 - Public- 1024 bits key
 - Private- 4096 bits key
- RSA addressed both the problems faced by the Diffie-Hellman algorithm by generating a set of private key and public key
- The receiving user could send the public key to all the senders to encrypt the data while keeping private key secret to themselves
- However RSA flaws for **commercial use**
- When designing the key, if the values of p and q are small then it can be decrypted just by random probability theory
- While if they are large then it consumes more time and performance degrades

Each cryptographic algorithm has weak points and strength points. We select the cryptographic algorithm based on the demands of the application that will be used. For our case RSA seems to be a relevant choice.

Technology Stack

1. E2EE Technique- We are going to use the RSA algorithm for end to end encryption.
2. Language For UI - Dart in Flutter framework.
3. Backend- Node.js
4. Socket library for real-time message exchange

Gaps in Research Papers

The Research Papers mostly addressed the various chat applications and what protocols they used. But,

-
- Maintainability of such applications was never addressed
 - The security details of different applications was only mentioned and not compared
 - Security problems faced by applications was not mentioned
 - Conversation integrity while chatting was not addressed in description of different applications

Research Papers

- [1] Nirvan Tyagi, Ian Miers and Thomas Ristenpart, "Traceback for End-to-End Encrypted Messaging", Published:06 November 2019, Available: <https://dl.acm.org/doi/pdf/10.1145/3319535.3354243>
 - [2] Katriel Cohn-Gordon, Cas Cremers, Luke Garratt, Jon Millican and Kevin Milner, "On Ends-to-Ends Encryption Asynchronous Group Messaging with Strong Security Guarantees", Published:15 October 2018, Available: <https://dl.acm.org/doi/pdf/10.1145/3243734.3243747>
 - [3] Paul Rosler, Christian Mainka, Jorg Schwenk, "More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema", Published: 09 July 2018, Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8406614>
 - [4] Wei Bai, Michael Pearson, Patrick Gage Kelley and Michelle L. Mazurek, "Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study", Published: IEEE 2020, Available: <https://eusec20.cs.uchicago.edu/eusec20-Bai.pdf>
 - [5] Michael Schliep and Nicholas Hopper, End-to-End Secure Mobile Group Messaging with Conversation Integrity and Deniability, published: November 11, 2019, available: <https://dl.acm.org/doi/pdf/10.1145/3338498.3358644>.
 - [6] Nina Gerber, Verena Zimmermann, Birgit Henhapl, Sinem Emeröz and Melanie Volkamer, "Finally Johnny Can Encrypt. But Does This Make Him Feel More Secure?", published: August 2018, Available: <https://dl.acm.org/doi/10.1145/3230833.3230859>
 - [7] Puneet Kumar Aggarwal, P.S. Grover, and Laxmi Ahuja, "Security Aspect in Instant Mobile Messaging Applications," published:23 August 2018 . Available: <https://ieeexplore.ieee.org/document/8443844> .
-