Advances in Artificial Intelligence Research (AAIR) **Vol. 1 (No. 2), pp. 52-59, 2021**
ISSN: 2757-7422
www.dergipark.com/aair **Published online: Aug 15, 2021**

Encryption Methods and Comparison of Popular Chat Applications

Muhammed Burak KILIÇ [1, *]

[1] Mugla Sıtkı Koçman University, Technology Faculty, Information Systems Engineering, Turkey
0000-0002-7503-9191

Abstract

In each period experienced in the field of communication as was the case in many areas of the peculiar and exceptionally experienced security problems brought by the era and continues to be experienced. However, in today's global world, this problem is accelerating day by day and increasing exponentially. Many data (photographs, videos, sound recordings) that should be kept confidential based on individual or society have become the limits with the developing technology. The purpose of the article is to propose end-to-end encryption provided chat applications where user individuals can exchange private information securely. The list of needed to develop a secure chat application has been presented in the article.

Keywords: *Secure chat applications; encryption methods; end-to-end encryption.*

1. Introduction

Although communication has been taking place in different forms since humanity existed, interaction is at its core. For instance, letters and telegrams have been replaced by text messages and e-mails with the widespread use of the internet. As the internet-based instant messaging applications provide more mobility than any other communication devices perhaps we can access, these applications have been increasing together with the constantly developing technology. According to Statista, a German company specializing in market and consumer data research, there are 41.9 million smartphone users in Turkey by 2018, and by 2025 this number will reach 72.5 million. [1]

Mobile devices have become an irreplaceable part of daily life with the rapid development of mobile phones. Correspondingly, chat applications have also developed and created a big change in social media in recent years due to their unique and special features that attract the masses. [2]

Users can easily share text messages, pictures, videos, and files using chat apps, which provide real-time messaging. Nearly all major messaging apps are currently available on Android and iOS operating systems and are being used by hundreds of millions of people. [3]

These applications have two different types. Which are client-server and peer-to-peer. P2P networks do not have a central server, and each user has their own data storage. [4] However, in the Client-Server network, data is stored on a central server. Client-Server network contains servers and clients used for processing. [4, 5]

Security and privacy are essential in these chat apps for all users; however, communities were far from actually what happened to their data and who could view those, until the WhatsApp Privacy Policy change on February 8, 2021. Encryption was initially thought to be paranoid or used by people with a high need for privacy. In reality, users have become more aware of the importance of data privacy and the dangers of identity theft after the revelations of hacker groups, and Edward Snowden, an American computer expert and former CIA and NSA employee. [6]

Accordingly, applications that have been around for years, research and updates to meet users' privacy, and demands in this direction have started to increase. Until the last few years, most applications have only used Transport Layer Security (TLS) to ensure security in special situations. As a result, the service provider was able to access any message it wanted. [7]

Therefore, these messages could also be accessed by attackers, so there was major security vulnerability. For this reason, to protect the confidentiality of messages, messages must be encrypted from sender to recipient, and the device's local storage must also be protected so that messages cannot even be read by service providers.

*Corresponding author
E-mail address: mdburakkilic@gmail.com

Received: 30/06/2021; Received in revised form: 01/08/2021; Accepted: 04/08/2021.

2. Cryptography

Cryptography is the science of ensuring the protection and security of the privacy of information. In our increasingly digital world, the encryption methods used for website or message/content security have their roots thousands of years ago. Although we define it as primitive today, the beginning of this science, which is still developing now, dates back to the early days when communication start to exist.

2.1. Encryption and Keys

Encryption is used to store or transmit data so that it can only be read and used by certain people. From the flat state it is, data can be encrypted or decrypted using symmetrical or asymmetric encryption systems that use one or more keys according to status and need to convert it to encrypted form.

The same key is used to encrypt and decrypt messages or data in symmetric encryption. Asymmetric encryption uses a public key as the encryption key and a private key to be used for the decryption solution.

2.2. Digital Signatures and Authentication

It is a cryptographic system used to verify the authenticity of data in a digital environment.

2.3. Key Exchange

It is a method by which encryption keys between two parties are securely exchanged, aiming to securely transmit messages or data using encryption.

3. Encryption Types

In modern encryption methods, two main encryption methods are often used. Symmetric encryption, where a single key is used to encrypt and decrypt the content, and asymmetric encryption, where secret (private) keys are used for public decoding for encryption.

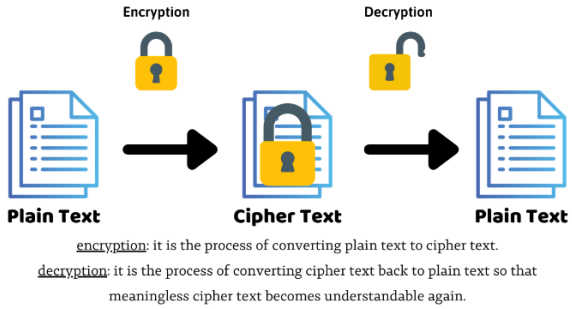

Figure 1. *Encryption and Decryption*

3.1. Symmetric Encryption

This type of encryption is the use of the same key or passwords to encrypt data or access the original state of encrypted data. For this type of encryption, the Secret Key is used to encrypt and decrypt the data. These secret keys are usually 128, 192, and 256 bits in size, but are also called encryption key or shared key because both the sender and the receiving party need to know. Most applications use certain existing passwords as keys, which is because it is easier for users to remember than data on the binary system. Modern cryptography symmetric encryption algorithms use AES (AES-128, AES-192, AES-256) as broadcasts.

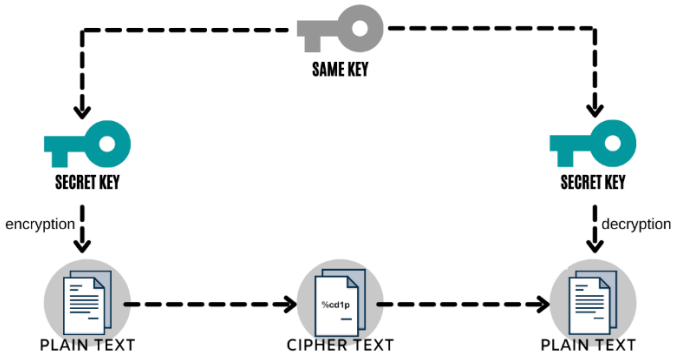

Figure 2. *Symmetric Encryption Structure*

3.2. Asymmetric Encryption

In asymmetric encryption systems, data is encrypted with a public key and used to decrypt and authenticate data encrypted with a private key. Data encrypted with a public key can only be resolved thanks to the corresponding private key. The data obtained after the encryption process is a binary sequence that cannot be read by individuals and cannot be decrypted by design without a decryption key.

Public key encryptions can typically encrypt limited-size messages, and symmetrical and asymmetric encryption can be used together for PDF or larger data or messages.

The most well-known methods for asymmetric encryption are RSA and ECC encryption methods.

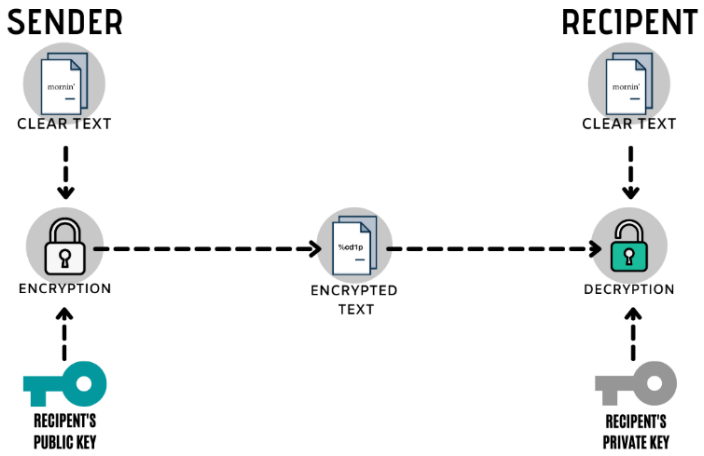

Figure 3. *Asymmetric Encryption Structure*

4. Encryption Algorithms and Methods

Modern encryption methods can be examined in different classes: symmetric, asymmetric and digital signature in key characteristics. For symmetric encryption, the sender and recipient share an encryption key and / or a decryption key. These two switches are usually the same or in case are easy to understand. There are two main standards for symmetric encryption. These are known as DES and AES. For asymmetric encryption, the receiving has a key and a private key. In this context, the public key can be shared, the private key must be kept private. Both RSA and ECC standards can be used in asymmetric encryption. In addition, the MD5 and SHA standards are included digital signature.

The encryption algorithms used are symmetrical, asymmetric, and hybrid (hash) encryption algorithms in which these two approaches are used together. Encryption techniques will make data more secure on the local system or the cloud system where it is stored.

AES: Advanced Encryption Standard is a symmetric key standard. Each of these passwords has a block size of 128 bits, with key sizes 128, 192, and 256 bits, respectively.

DES: Data Encryption Standard is the most widely used encryption algorithm. It works on one-size flat text blocks and is used to encrypt large data.

RSA: RSA is an algorithm used for public-key encryption which contains a public and private key. The public key here is known to the public and to encrypt submissions. Messages encrypted with a public key can only be decrypted using a private key. User data protected in this way includes pre-storage, retention or retrieval, authentication of users, and creation of secure channels for data transfer.

MD5: MD5 is an algorithm which can be used for encryption algorithms. With this algorithm, a variable-length message is like 128-bit fixed-length output. The input message is divided into 512-bit blocks; the message is filled in so that its length will be divided by 512. This sender uses a public key and the recipient uses a private key to decrypt the message.

ECC: Elliptic Curve Cryptography features modern public-key encryption systems based on the challenge of the elliptical curve discrete logarithm problem. ECC implements all of the asymmetric encryption system features of encryption, signatures, and key exchange. It is considered a more

modernized version of the RSA system, which is because the ECC uses smaller switches than RSA for the same level of the security process, resulting in much faster key generation and faster key interaction.

SHA: Secure Hash Algorithms define hash algorithms used in modern encryption. SHA-2 includes strong encryption hash functions: such as SHA-256, SHA-512, and so on. Legacy hash algorithms such as MD5, SHA-0, and SHA-1 contain cryptographic weaknesses. However, the SHA-2 family is considered extremely safe.

MD5, AES, ECC Hybrid Approach: Symmetric and asymmetric key encryption algorithms are used together to increase the level of security. In this approach, the actual data is encrypted with the MD5 algorithm, and the encrypted file is also encrypted by providing 3-level encryption with AES and then ECC.

5. Mobile Chat Applications

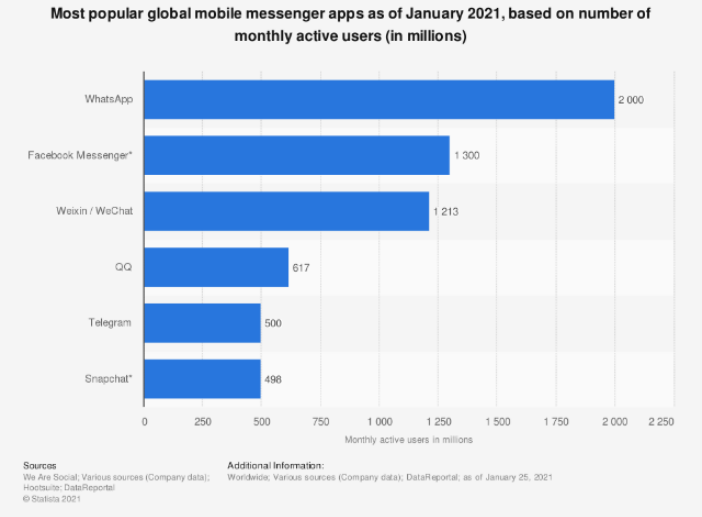

Figure 4. *The Most Popular Global Messaging Apps*

This section will include an overview of signal, WhatsApp, Telegram, Facebook Messenger, which are considered the best and most secure applications. [8]

5.1. WhatsApp

WhatsApp is now one of the most popular messaging apps globally with more than two and a half billion active users. [9] Messages between a sender and recipient using WhatsApp client software released after March 31, 2016 use the Signal protocol for voice and video calls. [10] Designed by Open Whisper Systems, this Signal Protocol forms the basis of WhatsApp's end-to-end encryption algorithm. This end-to-end encryption protocol is designed to prevent third parties other than the sender and receiver and WhatsApp from having direct plaintext access to messages or calls.

5.2. Signal

Signal was first used in 2010 to send encrypted messages and was developed by Whisper System's Moxie Marlinspike and Stuart Anderson and was known as a proprietary app under the name TextSecure. [11, 12] The Signal Protocol was developed by Open Whisper Systems in 2013. [13] This protocol, rooted in TextSecure, provides end-to-end encryption, and today WhatsApp [14], Facebook Messenger, and Signal applications also use it. [15] The application uses end-to-end encryption at the military level.

5.3. Telegram

Telegram, which was officially launched in 2013, is one of the most used and considered safe applications today. Telegram, which offers an open-source messaging service, uses its own cryptographic encryption protocol, MTProto. [16]

It supports two layers of secure encryption on its basis. Server-client encryption is used in cloud chats, i.e. private and group chats. Private chats use an additional layer of client-client encryption. It is

encrypted in the same way, regardless of text, media, or file type. Encryption operations are based on 256-bit symmetric AES encryption, 2048-bit RSA encryption, and Diffie-Hellman key exchange. [17]

5.4. Facebook Messenger

Facebook Messenger is a popular messaging service available for Android and iOS. It provides two messaging modes for normal (standard) chat and private chat (conversations). Standard chat uses only TLS, does not provide end-to-end encryption, and stores all messages on its servers. Messages in confidential conversations use Signal Protocol to provide end-to-end encryption between sender and recipient. Third parties other than speech – including Facebook – cannot access message texts and messages can only be decrypted by the requested recipient. [18]

Table 1. *Security and Privacy Features of Messaging Apps [19]*

Messaging App	End-to-end encryption	Private key not accessible by provider	Deleted from Server	Self-Destruct Messages	Open-Source	Password lock	Verification SMS/Email	Two-step Verification	Remote logout	Free
Line	✓						✓			✓
Messenger	✓(optional)			✓						✓
Signal	✓			✓	✓	✓				✓
Skype	✓(optional)									✓
Slack										✓
Snapchat	✓									✓
Telegram	✓(optional)	✓		✓	✓	✓		✓	✓	✓
Viber	✓	✓	✓	✓		✓				✓
WhatsApp	✓	✓				✓	✓			✓

6. Key Exchange and DHKE

6.1. Key Exchange

In cryptography, key exchange is a method by which keys are exchanged (exchanged) between two parties, thereby using an encryption algorithm.

If the sender and recipient want to exchange encrypted messages, each must be authorized to encrypt the messages to be sent and decrypt the received messages. The encryption that is needed depends on the technique that can be used as the basis. According to the encryption system, they will need different types of keys. If the password is a symmetric key password, both will need a copy of the same key. In asymmetric key encryption with public/private key capability, both will need the other's public key. [20]

By design, key exchange schemes securely exchange cryptographic keys between two parties so that no one else can access a copy of the keys. Key determination design occurs when a laptop connects to a wireless internet network or when a website is opened through a specific protocol. This key determination can be based on an anonymous key exchange protocol, a password, or the combination of many learning.

There are many cryptographic algorithms available for key exchange and key generation. Some of these algorithms use open-key encryption systems, some use simple key exchange methods, some may include server authentication, and some may include client authentication. This article will include one of the first public-key protocols, the Diffie-Hellman Key Exchange.

6.2. Diffie-Hellman Key Exchange

The Diffie-Hellman key exchange algorithm, the first public-key algorithm announced, is based on the process of safely changing a key between two users over a public (unsafe) environment. Since the DH method is an algorithm that only provides key exchange, keys changed after the process are then used for encrypted communication.

At its core is the process of generating public secret keys that can be used in secret communications. This key also ensures secure data exchange on public (untrustworthy) networks.

For a better understanding of the Diffie-Hellman Key Exchange protocol, we can use the key exchange visual sample by mixing the best-known colors. (Figure 5)

The design of the color mixing and key change scheme proceeds on the assumption that if there are two different colors, we can easily mix these colors and make a new color. Reversal is almost impossible, as there is no clear management or way to parse mixed colors into their original colors.

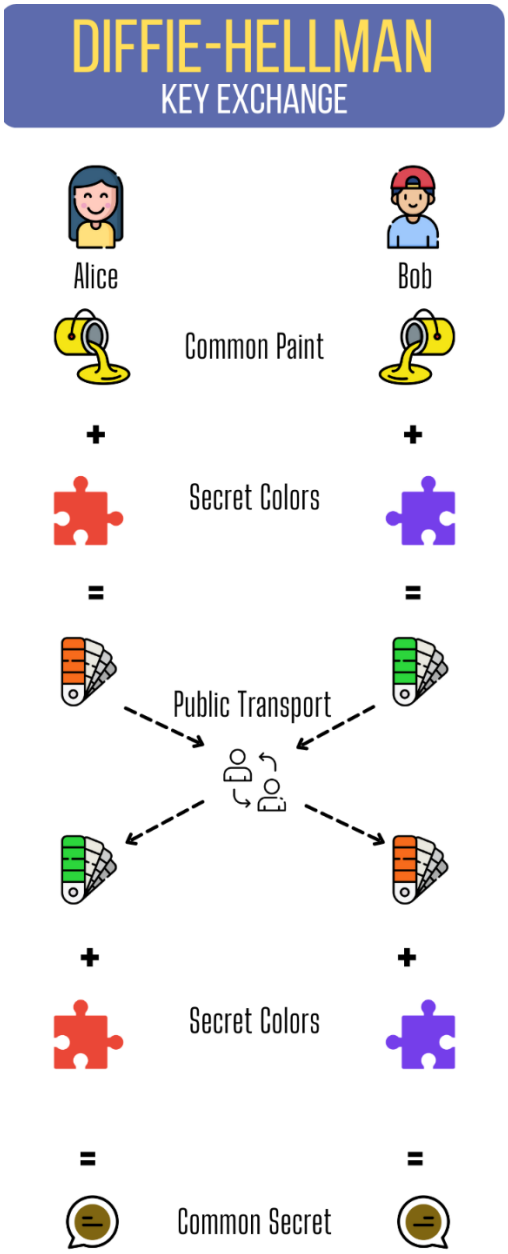

Figure 5. *Diffie-Hellman Key Exchange Algorithm*

To explain with a classic example:

Alice and Bob identify a common color between them that is accessible to everyone. In our example, let's consider the color yellow.

Then they choose a hidden color that only they know. (red and blue)

This hidden color is mixed with the common color originally specified, and the resulting new colors are exchanged in a way that is also accessible to third parties. This does not cause security weaknesses because there is no easy and effective way to parse these mixed colors.

Finally, Alice and Bob mix the color they get from each other with the hidden color they set themselves, and as a result, they get a common color. The common color obtained as a result of the operations represents the common secret between them.

Even if the color changes made explicitly are known, the probability of access to the color at the end of the process is very low because the hidden colors determined by the users are unknown. In the Diffie-Hellman Key Exchange method, modular bases are used instead of color, which is one of the reasons why this process is safe.

7. Result and Recommendations

In this study, the definition and how terms such as encryption and key, digital signature, and key exchange are used for cryptography and then cryptography are discussed. Then there is the structure and functioning of symmetrical and asymmetric encryption algorithms, the two main types of encryption used for modern encryption operations.

Symmetric encryption is an encryption method in which the sender and receiver use a public key for both encryption and decryption. Although encryption is faster with this method, it can cause a number of security vulnerabilities because the sender and recipient will need to securely change their keys. AES and DES are popular standards for symmetric encryption.

Asymmetric encryption uses two different keys to encrypt and decrypt data. One key here is used for encryption, while the other is a common key-based encryption method that is used to decrypt. Where the sender encrypts the message with the public key, the recipient uses the private key created to decrypt the same password. To protect privacy and authentication, encryption is based on the rule that the public key does the encryption and decrypts with the help of the private key. RSA, ECC, and DHKE are frequently used, popular public-key encryption systems.

Based on the algorithms used after basic encryption methods, comparisons of existing popular chat applications and their chat and data security features are included.

In the study, the DHKE method was mentioned and information about its structure and functioning was given. The Diffie-Hellman method is based on the key exchange structure and is the first open key algorithm announced. This key exchange algorithm is a method used to change cryptographic keys securely or confidentially.

References

[1] J. Degenhard, «Forecast of the number of smartphone users in Turkey from 2010 to 2025,» 2021. [Çevrimiçi]. Available: https://www.statista.com/forecasts/1146422/smartphone-users-in-turkey.

[2] A. Read, «How Messaging Apps Are Changing Social Media,» 2016. [Çevrimiçi]. Available: https://blog.bufferapp.com/messaging-apps.

[3] H. Tankovska, «Most popular global mobile messenger apps,» 2021. [Çevrimiçi]. Available: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/.

[4] N. Sabah, J. M. Kadhim ve B. N. Dhannoon, «Developing an End-to-End Secure Chat Application,» International Journal of Computer Science and Network Security, no. 17, pp. 108-113, 2017.

[5] D. Moltchanov, «Client/server and peer-to-peer models: basic concepts,» Department of Communications Engineering, Tampere University of Technology, 2013.

[6] B. Muqeet, «Best Secure Messaging Apps for Android and iOS,» 2018. [Çevrimiçi]. Available: https://www.privacyend.com/best-encrypted-messaging-apps/.

[7] M. Kleppmann, «The Investigatory Powers Bill would increase cybercrime,» 2015. [Çevrimiçi]. Available: https://martin.kleppmann.com/2015/11/10/investigatory-powers-bill.html.

[8] C. Corrigan, «The Very Best Encrypted Messaging Apps,» 2020. [Çevrimiçi]. Available: https://www.avg.com/en/signal/secure-message-apps.

[9] M. Iqbal, «WhatsApp Revenue and Usage Statistics (2021),» 2021. [Çevrimiçi]. Available: https://www.businessofapps.com/data/whatsapp-statistics/.

[10] WhatsApp, «WhatsApp Encryption Overview [Technical white paper],» 2020.

[11] C. Garling, «Twitter Open Sources Its Android Moxie,» 2021. [Çevrimiçi]. Available: https://www.wired.com/2011/12/twitter-open-sources-its-android-moxie/.

[12] A. Greenberg, «Android App Aims to Allow Wiretap-Proof Cell Phone Calls,» 2010. [Çevrimiçi]. Available: https://www.forbes.com/sites/firewall/2010/05/25/android-app-aims-toallow-wiretap-proof-cell-phone-calls/.

[13] K. Ermoshina, F. Musiani ve H. Halpin, «End-to-End Encrypted Messaging Protocols: An Overview,» %1 içinde International Conference on Internet Science, Floransa, 2016.

[14] WhatsApp, «WhatsApp Encryption Overview,» 2020. [Çevrimiçi]. Available: https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf.

[15] Facebook, «Secret Conversatiıns,» [Çevrimiçi]. Available: https://www.facebook.com/help/messenger-app/1084673321594605/.

[16] Telegram, «Security,» [Çevrimiçi]. Available: https://telegram.org/faq#security.

[17] Telegram, «Telegram FAQ,» [Çevrimiçi]. Available: https://telegram.org/faq#q-so-how-do-you-encrypt-data. [Erişildi: 2021].

[18] Facebook, «Messenger Secret Conversations [Technical white paper],» 2017.

[19] J. Botha, L. Leenen ve C. Van ‘t Wout, «A Comparison of Chat Applications in Terms of Security and Privacy,» %1 içinde 18th European Conference on Cyber Warfare and Security, 2019.

[20] Wikipedia, «Key exchange,» [Çevrimiçi]. Available: https://en.wikipedia.org/wiki/Key_exchange.

[21] Statista, «Most popular global mobile messenger apps as of April 2021, based on number of monthly active users,» 2021. [Çevrimiçi]. Available: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/.