SCIENCE AND INNOVATION
INTERNATIONAL SCIENTIFIC JOURNAL VOLUME 1 ISSUE 8
UIF-2022: 8.2 | ISSN: 2181-3337

DEVELOPMENT OF SECURE MODELS AND ALGORITHMS OF MESSENGERS WHEN EXCHANGING SERVICE MESSAGES

Karimov M.M.
Director of the State Test Center under the Cabinet of Ministers of the Republic of Uzbekistan
G`ulomov Sh.R.
Dean of the Faculty of Cyber Security of Tashkent University of Information Technologies named after Muhammad al-Khorazmi,Uzbekistan
Eshniyozov T.T.
Master's degree, Faculty of Cyber-Security,Tashkent University of Information Technologies named after Muhammad al-Khwarizmi,Uzbekistan

https://doi.org/10.5281/zenodo.7444932

Abstract. *Today data communication is a modern technology that contains a powerful computer processor to exchange information. But brute force attacks are made to break the encryption techniques and these attacks are the main drawbacks of older algorithms. This paper is concerned with the development of a secure messaging system based on cryptographic algorithms that is which is more faster, better immune to attacks, more complex, easy to encrypt and many more advanced security feature included. This project work is designed and developed for a secure messaging both in web and android platforms. The application is well featured and provides encryption/decryption that can protect message from unauthorized access and disclosure over networks. To send message, a recipient or registered user types and encrypts a text message using keyword mono-alphabetic substitution algorithm with a key, selected from key list. The encrypted message is stored in the database and receiver's inbox with serial number of key (not the value). The receiver, after log into his/her own account, selects the key value and then decrypts the encrypted message with the key to see the original message. With compared to other messaging systems, the proposed secure messaging system can be used for chat, messaging, video conferencing and real time file sharing in both web and android platforms.*

Keywords: *Secure messaging; Cryptography; Encryption; Decryption; Web application; Android apps*

РАЗРАБОТКА БЕЗОПАСНЫХ МОДЕЛЕЙ И АЛГОРИТМОВ МЕССЕНДЖЕРОВ ПРИ ОБМЕНЕ СЛУЖЕБНЫМИ СООБЩЕНИЯМИ

Аннотация. *Сегодня передача данных — это современная технология, которая содержит мощный компьютерный процессор для обмена информацией. Но атаки грубой силы совершаются для взлома методов шифрования, и эти атаки являются основными недостатками старых алгоритмов. Эта статья посвящена разработке защищенной системы обмена сообщениями на основе криптографических алгоритмов, которая является более быстрой, более защищенной от атак, более сложной, простой в шифровании и включает в себя множество дополнительных функций безопасности. Этот проект разработан и разработан для безопасного обмена сообщениями как на веб-платформах, так и на платформах Android. Приложение хорошо оснащено и обеспечивает шифрование/дешифрование, которое может защитить сообщение от несанкционированного доступа и раскрытия по сети. Для отправки сообщения получатель или зарегистрированный пользователь набирает и шифрует текстовое сообщение с использованием алгоритма моноалфавитной замены ключевого слова ключом, выбранным из списка ключей. Зашифрованное сообщение сохраняется в базе* *данных и в почтовом ящике получателя с серийным номером ключа (а не значением). Получатель после входа в свою учетную запись выбирает значение ключа, а затем расшифровывает зашифрованное сообщение с помощью ключа, чтобы увидеть исходное сообщение. По сравнению с другими системами обмена сообщениями предлагаемая система безопасного обмена сообщениями может использоваться для чата, обмена сообщениями, видеоконференций и обмена файлами в реальном времени как на веб-платформах, так и на платформах Android.*

***Ключевые слова**: безопасный обмен сообщениями; Криптография; Шифрование; Расшифровка; Веб приложение; Приложения для Android.*

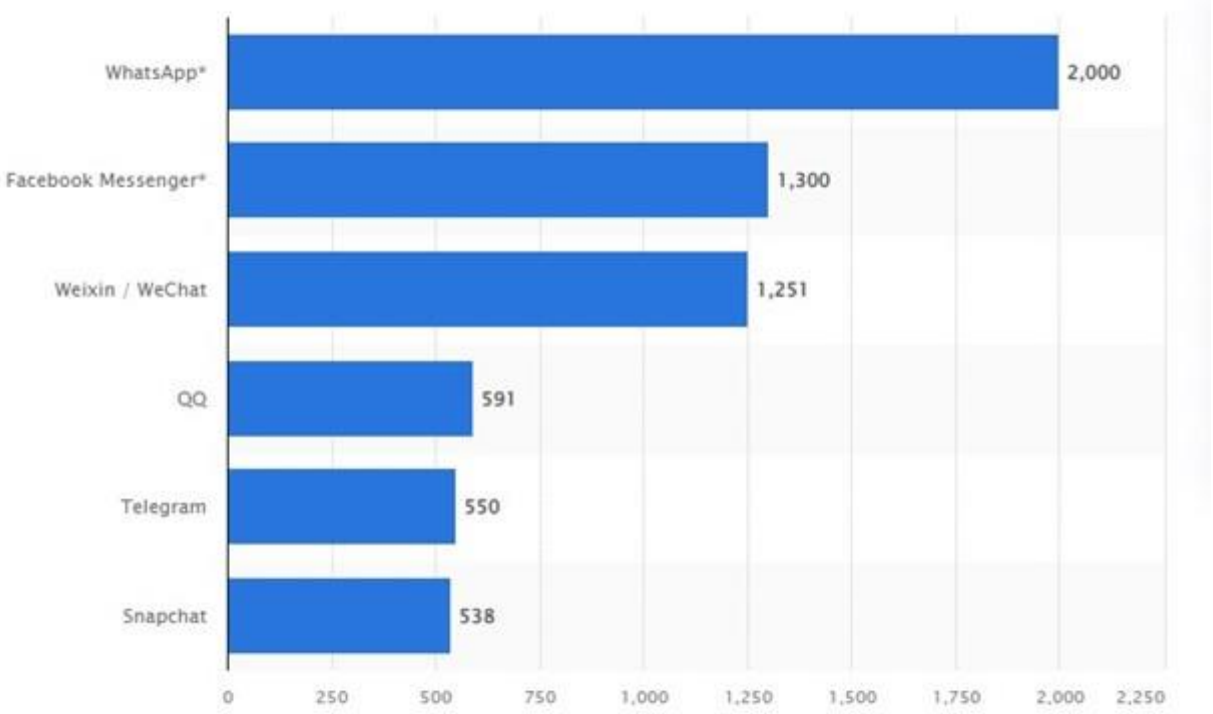
Introduction. Technology is used in every sphere of life and people are more dependent on Smartphone technology that contains a powerful computer processor to exchange data information. This is because of necessity of our multimedia documents to be protected from unauthorized person. So a day-to-day use of cryptography in our life is increasing tremendously. Messaging system is a text or instant messaging service component of phone, web, or mobile communication systems over the world. But is it really safe to use? Recently the Electronic Frontier Foundation (EFF) has submitted a report that is not comfortable for all users. Because we have to rely as much of our personal information while chatting in fact it is not safe to write there. The public instant messaging systems, the messages are travel from the client to the server and back to the second client. This data is potentially visible to eavesdroppers anywhere along its Internet path or within the network. So the information at any moment it could have gone to someone else. For this reason, this project work is concern with the development of secure messaging system using cryptographic technique.

Materials. Symmetric-key cryptosystems use the same key for encrypting and decrypting message in network security. A significant disadvantage of symmetric encryption is the key management necessary to use them securely. In a groundbreaking 1976 paper, Whitfield Diffie and Martin Hellman proposed the notion of public-key cryptography in which two different but mathematically related keys are used; a public key and a private key. A public-key system is so constructed that calculation of one key (the 'private key') is computationally infeasible from the other (the 'public key'). Instead, both keys are generated secretly, as an interrelated pair. The historian David Kahn described public-key cryptography as "the most revolutionary new concept in the field since polyalphabetic substitution emerged in the Renaissance". An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

Methods. Encryption is the process of transforming plaintext data into something that appears to be random and meaningless, known as cipher text. Decryption is the process of converting cipher text back to plaintext. To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of cipher text, the key that was used to encrypt the data must be used. There several types of operations used for encryption and decryption. Substitution and transposition ciphers are two categories of ciphers used in classical cryptography. All encryption algorithms are based on these two principles. In substitution, each element in the plain text is mapped into another element, and in transposition, the plaintext are rearranged. Most systems referred to as product systems, involved multiple stages of substitution and transposition. Substitution and transposition differ in how chunks of the message are handled by the encryption process. There are different types of substitution cipher. If the cipher operates on single letter, it is termed a simple substitution cipher; a cipher that operates on a group of letters is termed polyalphabetic. A mono-alphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different positions in the message, where a unit from the plaintext is mapped to one of several possibilities in the cipher text and vice versa. The cryptographic algorithm with keyword mono-alphabetic cipher has been used in this project work.

Results. The transfer of information via instant messengers has long become an integral part of our everyday life. Messengers allow you to quickly and easily interact with others on a variety of issues such as work, education, entertainment, and personal contacts. The functions of modern messengers have gone beyond the usual exchange of messages, photos, and videos. We can make audio and video calls, shop, pay utility bills, get help, order food, taxis, tickets, and more.

WhatsApp is minimalistic and functional. Certain shortcomings in the areas of security and privacy do not prevent it from being the most popular instant messenger in the world. The web version and desktop support also make up for many of the security concerns. The app leverages end-to-end encryption by default, which is often discussed by online communities of privacy-minded users. Backups are not encrypted.



The development of cloud technologies has also increased the influence of instant messengers on our lives, as it is really convenient when important files, correspondence, and contacts are at hand and so easy to share.

We are so used to all this that we completely fail to notice the amount of confidential information that we send through instant messengers every day. Numerous and various scandals and bugs associated with popular messengers make us wonder whether our messenger of choice is secure enough? Is our data encrypted in the cloud and who has access to this data? How to evaluate the security of a messenger in general?

Let's try to assess the privacy of messengers marketed as safe in terms of certain key parameters and try to answer the question: which messenger currently provides the best user privacy?

Threats and Risks: The threat model will be highly personalized because we are dealing with personal data. Each user has to figure out what exactly needs to be protected. Is it correspondence, content, identity, metadata, or location? Odds are that all of the above. Who may abuse the data? Do we want to keep our data safe from advertising companies, the government, and hackers? What about family members?

Each scenario has its undercurrents, which is important to take into account. Here is some extra food for thought: a service that effectively protects your messages and metadata could be less suitable, for example, for entertainment and may be inconvenient for everyday use.

Data Leaks: Gaining unauthorized access to confidential information your messenger generates and stores (by intercepting messages in real time, accessing message logs, extracting data from the cloud, or authenticating behind your back) will lay the groundwork for a number of extremely unpleasant attacks with unpredictable consequences. This can be blackmail, impersonation of a confidant, or data collection for implementing more complex schemes using social engineering.

Location Disclosure: When the function of sharing the current location is activated, or if the messenger allows you to reveal your mobile number, an attacker can piece together your daily schedule of presence in a particular location. The malefactor can use these personal routes of movement to orchestrate an attack or sell this data to third parties.

Code Vulnerabilities and Compromised Software: Like any software, a messenger may contain vulnerabilities that facilitate access to more than just confidential information. Installing a compromised application, such as one from an untrusted source, can lead to a more serious attack. As a result, a malicious actor can gain complete control over the device and go unnoticed. It must be understood that as soon as an attacker takes over a messenger account, this does not lead to anything good. Even if the account does not contain any valuable information, it can be added to a botnet and weaponized in DoS attacks, spam campaigns, the distribution of malicious links, etc.

Criteria for the Security and Privacy of Messengers: To gauge the security of user data in a particular messenger, we need to denote the key benchmarks regarding security, privacy, and anonymity. Since modern applications run in a sandbox and leverage various behavioral controls, a lot comes down to how the logic of the application is organized in a particular platform.

End-to-End Encryption: End-to-end encryption support ensures that only you and the recipient can decrypt and read the information. E2E is considered the main attribute of any messenger that positions itself as secure. An important point to consider is whether this option is enabled by default. For example, in iMessage, until recently, encryption had to be manually activated in the settings.

It is also important to understand what cryptographic algorithms are used to perform encryption. Where is the private key generated? Is the metadata hashed? Is there a key rotation process in place?

Data and Metadata Harvesting: The metadata that each of us generates through our online activities is like a digital fingerprint. Messengers also collect metadata that can describe our personality in great detail. In fact, this is all the data besides the content of the message itself: for example, whom from our contact list we talk to, how long and how often (sender, recipient, time sent, time read). This is a kind of record of our activity. Information about the device used, IP address, and mobile number may also be harvested.

That's nothing but the collection of data about users in its purest form. At a minimum, these are details provided during registration. In some cases, it is difficult to determine exactly what data is collected, because instant messengers are integrated into the ecosystem of the manufacturer (Google Messages, Apple iMessage). Companies may know the user ID, phone number, content of correspondence, search history, browsing history, purchase information, location, contacts, and more.

Open Source: An open-source instant messaging application allows comprehensive security auditing. Hobbyists, enthusiasts, and experts can build an application, examine its operation, and draw attention to weaknesses, vulnerabilities both in the server and client parts of the code. On the other hand, free access to the code slightly increases the risk that information about a discovered vulnerability can be used with malicious intent until it is closed or someone else from the community pays attention to the weakness. Open-source code per se cannot guarantee the security of user data, but it definitely contributes to this condition.

Sharing Data with Third Parties: Third parties may be special services, public order authorities, or government agencies. The administration of some messengers actively cooperates with such entities, while others consistently reject personal data requests. An attacker can pretend to be any person you can imagine, including a member of the special services, and as a result receive the necessary valuable information. When choosing a secure application, this must be taken into account, otherwise your confidential data may be abused, even if you are a law-abiding citizen.

Encryption of Backups in the Cloud: Not all messengers use encryption to store correspondence and files in the cloud. A successful attack by a hacker on the cloud infrastructure can lead to the leakage of confidential data. As is the case with data collection, information about whether the backup is actually encrypted is not publicly available on all messengers.

Peer-to-Peer Connection Support: Peer-to-peer connection excludes any third party involvement. Messages stream directly to the recipient's device. There is a caveat, though: a connection like that reveals with whom and for how long it has been established, which, of course, affects anonymity and reduces the level of confidentiality. You can step up your privacy by implementing additional protection of the IP address through the use of a VPN or Tor.

Sign-up Data: Creating an account with a messenger often requires us to provide a mobile phone number, which is closely related to our identity. Data security may not be affected, but anonymity suffers badly. The more data is required during registration, the lower the anonymity. Email address might suffice, or the application may request access to contacts or incoming SMS messages for verification. To complete registration, the app may request a call to your number.

Other Security Features: Two-factor authentication (2FA) support is an important additional security element. The second layer of protection based on 2FA can effectively stop intruders in their tracks. Some applications prompt the user to activate 2FA through a notification. This typically goes bundled with the following:

an option that allows you to set a code or a passphrase to access important security settings or sensitive chats; protect information displayed on the screen (for example, when a user tries to take a screenshot of secret messaging, the person on the other end receives a notification about this);

automatic screen lock when the user moves away from the device;

deleting a previously linked device from the account, etc.

So, How Secure Are the World's Top Messengers?

Now that we have set the evaluation criteria, let's identify the most reliable of the 13 most popular instant messengers marketed as safe: Apple iMessage, Element/Riot, Facebook Messenger, Google Messages, Microsoft Skype, Session, Signal, Wire, Telegram, Threema, WhatsApp, Viber, and Wickr Me.

Outsiders: Let's start with outsiders. It is definitely worth paying attention to these applications and thinking about what is happening not only with our personal data, but also with privacy: Apple iMessage, Microsoft Skype, Google Messages, WhatsApp, and Facebook Messenger. This does not mean that these messengers cannot be used, because here we once again return to the formation of a personal threat model and the goals that we pursue in building security.

All outsiders, with the notable exception of WhatsApp, are built into their respective closed ecosystems through which a striking amount of our personal data flows. If we use services from Google or Apple, these corporations have already collected all the necessary data about us even without instant messengers.

Best in Terms of Security and Privacy: Session, Signal, Threema, and Wickr Me are undoubted leaders in security and privacy.

Session has been gaining popularity since 2020 due to decentralization and the use of end-to-end encryption based on the Signal protocol. The messenger features anonymous registration in one click without entering passwords. It uses a bare minimum of metadata when sending messages. The weak points are that calls are not currently supported, and in some cases, messages may be delivered with a noticeable delay.

Signal is very good in terms of security and functionality, but there is a drawback that seriously affects privacy as anonymous registration is not supported, so you will have to entrust your mobile phone number to the messenger. Among other options, Signal enables automatically blurring people's faces on all photos sent to the chat.

Threema is a secure but paid messenger. It stores correspondence on the server, and the registration is fully anonymous.

Wickr Me supports anonymous registration as well. Your correspondence gets encrypted and stored on the server for 30 days. You will also need to wait for 24 hours until your account is deleted from the system. But otherwise, it is by far the best choice, combining proper security and privacy.

Golden Mean: The best options for everyday secure and convenient communication are Element (formerly Riot), Telegram, Viber, and Wire.

Element is a well-known secure messenger with a full range of features for daily communication. The disadvantage is the lack of two-factor authentication; in addition, some privacy features could use some enhancements. That being said, anonymous registration is available offsetting the above and other drawbacks.

Telegram does not support end-to-end encryption by default, which is one of the key drawbacks. The secret chat feature needs to be activated. Anonymous registration is not supported. The messenger has very flexible privacy settings, and its user-friendly desktop version wins it an extra audience.

If you use Viber, beware the messenger collects a lot of personal data. If that doesn't bother you, Viber is a great choice. Desktop and mobile applications are equally good and convenient for communication. End-to-end encryption is supported by default.

Wire offers a streamlined design for the mobile app and desktop version. It's a neat combination of security and convenience. Compared to Telegram, it has slightly fewer privacy settings but uses end-to-end encryption by default. Backups are stored on the device only.

Convenience in Exchange for Security: If you prioritize convenience when choosing a messenger and leave the security and privacy of personal data aside, consider using the following products.

Facebook Messenger is almost as popular as WhatsApp simply because it is embedded into Facebook. It's no secret that Facebook collects a huge amount of users' personal data for its own benefit. End-to-end encryption is not enabled by default. If you are an active user of the most popular social network in the world, this messenger will allow you to quickly and conveniently keep in touch with your Facebook friends list.

Microsoft Skype is the legendary messenger for audio and video calls. Its encryption algorithms are a far cry from being the most reliable, but users appreciate multifunctional conferences with the ability for all participants to record and quickly receive a broadcast file. It is also worth highlighting the support for both mobile and desktop versions. For many years, Skype has been one of the most popular messengers for communication across the board.

Conclusion. In terms of personal data security and privacy, Signal, Threema, and Wickr Me are the top messengers. However, each service has its pros and cons. The ideal application in terms of absolute security and anonymity of secure instant messaging has yet to be created.

It is impossible to provide high anonymity without sacrificing other features. For example, the speed of message delivery in a more secure messenger is significantly reduced, there is a limit on the size of an attachment, etc. That being said, when choosing a messenger for everyday communication, an ordinary user should find a reasonable trade-off between convenience and security.

The main objective of the proposed system is to transfer message in a communication system securely. Android-based and webbased applications for secure messaging have been developed using cryptographic algorithms for the users to send their message between registered users on any organization securely. The application is supported through user authentication before sending message. The proposed secure messaging system uses minimal processing with little overhead while maintaining security. The authentication of each user is made strong by storing sensitive credentials for each user by using Salt in the database. Encryption and decryption of message are done by using keyword mono-alphabetic substitution algorithm, which is based on Advanced Encryption Standard (AES). This is less secure than the public-key encryption scheme. This is main limitation of this work. An eavesdropper that breaks into the message will return a meaningless message. Obviously encryption and decryption is one of the best ways of hiding the meanings of a message from intruders in a network environment. The proposed secure messaging can be used in many areas with personal and company-wide sensitive data exchanges. For example, financial institutions, insurance companies, public services, health organizations and service providers rely on the protection by Secure Messaging. It is concluded that the developed application can be considered for chat, messaging, video conferencing and real time file sharing in these application areas. The proposed system has been designed and developed with easy integration and modification to take full advantage of future technologies. There are some limitations in the current system to which solutions will be provided as a future development; such as, small number of keywords uses only keyword mono-alphabetic substitution algorithm and network bandwidth. In future, a public-key encryption scheme will be implanted in secure messaging system.

REFERENCES

1. Rivest RL Cryptology. Handbook of Theoretical Computer Science.
2. https://www.eff.org/secure-messaging-scorecard.
3. Paar C, Pelzl J, Preneel B (2020) Understanding Cryptography: A Textbook for Students and Practitioners. Springer.
4. Liddell HG, Scott R, Jones H, McKenzie R (2018) A Greek-English Lexicon. Oxford University Press.
5. Diffie W, Hellma M (2016) New Directions in Cryptography. IEEE Transactions on Information Theory 22.
6. Schneier B (2017) Cryptanalysis of MD5 and SHA: Time for a New Standard. Computerworld.
7. Diffie W, Hellman M (2016) Multi-user cryptographic techniques. AFIPS Proceedings 45: 109-112.
8. Kahn D (2019) Cryptology Goes Public. Foreign Affairs.
9. Goshwe NY (2018) Data Encryption and Decryption Using RSA Algorithm in a Network Environment. IJCSNS International Journal of Computer Science and Network Security 13.
10. William Stallings (2016) Cryptography and Network Security Principles and Practices. Pearson Education Inc.
11. The Text Message Turns 20 (2020) CNN.
12. Federal Information Processing (2019) Announcing the ADVANCED ENCRYPTION STANDARD (AES).
13. James McCarey, Keeping Your Data Secure with the New Advanced Encryption Standard. MSDN Magazine.