Encryption Techniques for Different Messenger Applications

Maganti Manasa, Dasari Veera Reddy, AmanapuYaswanth, G.V.S Raj Kumar

***Abstract:** With the advancements in number of technologies, communication has taken a bigger leap. A number of messenger applications have been developed to exchange data and information through the Internet. This data is very private and can be vulnerable to security attacks. Hence, it must be protected with certain encryption technique to keep the information confidential and away from unauthorized access. In this paper, a brief study is done on different encryption techniques in messenger applications and the conclusions are presented.*

***Keywords:** Cryptography, Encryption, hashing algorithms, messenger applications, symmetric and asymmetric key cryptography*

I. INTRODUCTION

The subject of Cryptography has always been an important field of research. It has established its mark in field of IT as security has always been an issue of concern. From storing the data in the servers to exchanging the multimedia, security plays an important role. It involves encrypting the data at sender's (Alice) end and decrypting it at the receiver's (Bob) end. An original message that is sent by sender is known as the Plaintext. The text which is coded is known as the Ciphertext. Encryption is the process of converting the plaintext to ciphertext. Decryption is the process of obtaining the plain text from cipher text. The cryptographic system works in two ways. In public key cryptosystem, two keys are used where private key stays with the sender and the public key is accessible to all the members in the network. In symmetric key cryptography, the data is sent from sender to receiver and same key is used for both encryption and decryption. Various encryption algorithms have been developed through years such as DSA, AES, RSA, Diffie-Hellman, Elliptical curve etc. Along with these algorithms, also hashing algorithms such as SHA-1, SHA-256, MD5 HMAC etc. have been developed to enhance the standard of encryption. A few messenger applications are taken into consideration and their encryption standards are studied and efficiencies are presented.

Revised Manuscript Received on December 13, 2019.

***** Correspondence Author

Maganti Manasa*, UG Student, GITAM, Visakhapatnam, India, Email:manasamaganti99@gmail.com.

Dasari Veera Reddy, Asst.Professor in Computer Science and engineering, GITAM, Visakhapatnam, India.Email:dasariveerareddy01@gmail.com.

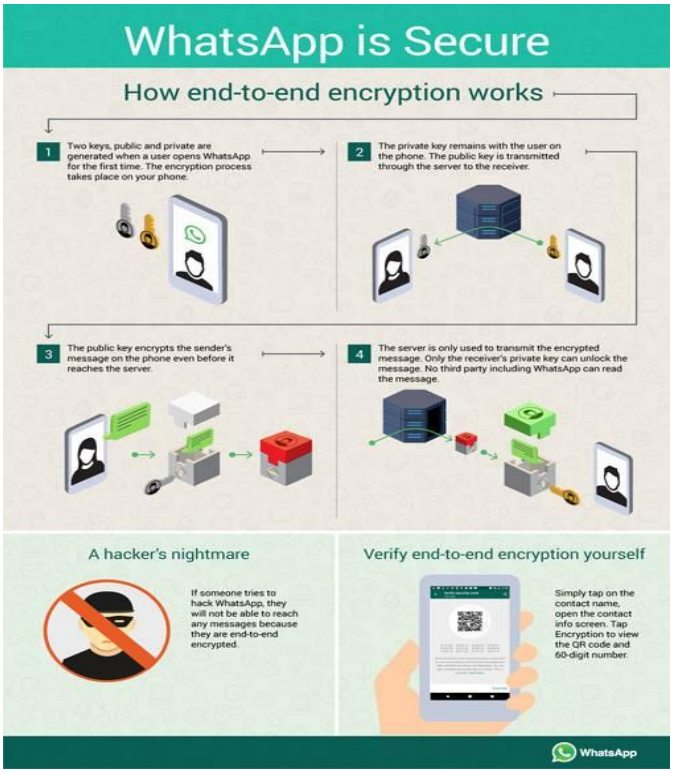
Amanapu Yaswanth, Asst.Professor in Computer Science and Engineering, GITAM, Visakhapatnam, India. Email:yashmtech@gmail.com.

G.V.S Raj Kumar,Professor in Computer Science, and Engineering, GITAM,Visakhapatnam, India. Email:gvsrajkumar.ganapavarapu@gitam.edu

II. METHOD

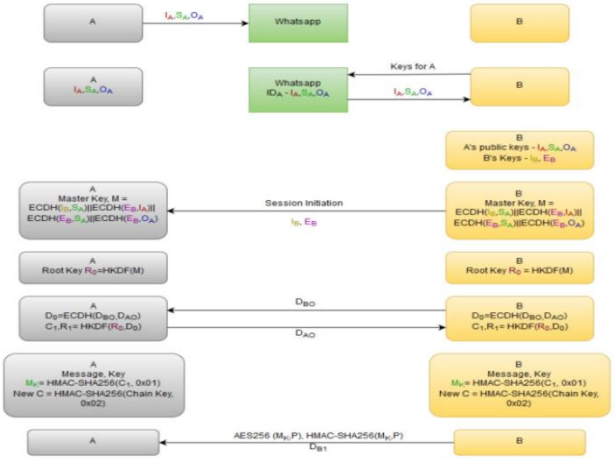
WhatsApp

WhatsApp being one of the most commonly used messenger appsthat has about user base of 200 million people. Billions of messages are sent each day through this application. Initially this app was designed with a motive to send free message services to the people and hence there was no encryption standard. The information was sent in the form of plain text messages from sender to receiver. This led to security breach in the application and WhatsApp faced quite a few allegations for this. However, to overcome this problem, WhatsApp added its first encryption standard in 2012. A 256-bit algorithm was used for encryption which had brought up a level of security to the application.



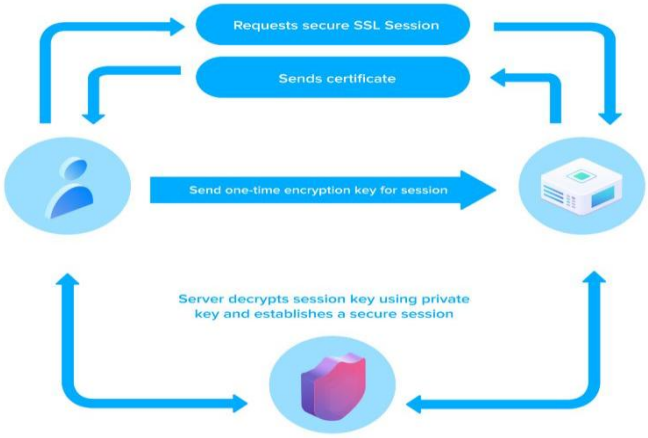
In addition to this, WhatsApp has introduced a new end-to-end encryption standard in the year 2016 which was widely appreciated across the world. Due to this feature, it has gained appraisal from the Electronic Frontier Foundation's "Secure Messaging Scorecard". WhatsApp uses a combination of both symmetric and asymmetric key cryptographic algorithms. It uses the signal protocol called "Text Secure" which basically safeguards and maintains the integrity and confidentiality aspects of the algorithm.

This protocol is built on a set of cryptographic primitives which uses Diffie Hellman Key exchange over Elliptical-Curve (ECDH) and Curve25519 is used in native cryptographic library. It also uses AES-256 with counter mode for symmetric encryption and HMAC-SHA256 for message integrity. Once the encryption is done, it proceeds with the signature which ensures the end-to-end encryption.



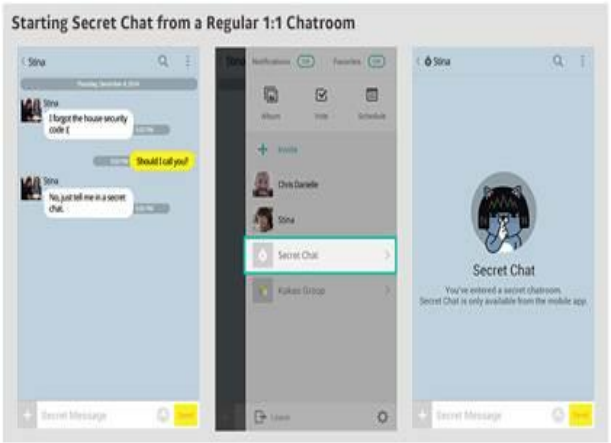
Hike Messenger

One of the most popular messenger applications in India which is used for instant messaging, image sharing, video chatting and multimedia. With many features like Hike news, offline SMS, hidden mode, etc., in this application, it has gained majority of its user base from young audience. When hike was initially released in the year 2012, it allowed only free messaging services with sticker chat. There was no such encryption standard for the messages that were sent over the net. There were many loopholes when the app was tested on privacy basis. Some of these include transmission of contacts from phonebook, getting access to the unique device identification number. However, Hike considering all these ambiguities launched a new encryption feature for messages. This uses a 128-bit Secure Socket Layer which is encrypted with the Firewall server. This symmetric encryption technique is considered as one of the most secure algorithms that is logically unbreakable. It might take a million years to crack the information that is being sent. Although it has obtained a significant amount of security with SSL, it has been still working on improving the privacy with new encryption techniques. The latest security update includes encryption of chats and calls with 128-bit AES and 2048 RSA public key cryptosystems. With all its servers in India, it does not allow security breach to third party apps. In addition to messenger services, Hike has also introduced the Hike web service where communication can be established over PCs. It has ensured the network security for Hike web using AES-256 that protects the data from security attacks over the web. These algorithms which are used for encryption stores the data of messenger application by keeping the key and salt in two different management systems.



KakaoTalk`

KakaoTalk is one of the leading messenger app in South Korea with 90% of users using the smart phone. It was initially released in 2010 with its compatibility with wide range of operating systems. Along with chats and calls, multimedia sharing is also available on the platform. During its initial release, the app did not have any encryption technique as such. The drawback to this model was these chats were not backed up and were lost when signed in through a new device. This had led to new encryption technique where the data is summarized in the form of a .db file and is backed up in the cloud. Furthermore, the secret chat mode was released to use end-to-end encryption on all messaging services. However, the size of the database file was limited to 20MB and hence most of the heavy data files were lost. While performing the encryption and decryption in KakaoTalk, it was found out that AES-128-bit encryption in CBC mode was used as means of encryption for these database files. In Jusop Choi et al. they have clearly mentioned about the procedures to generate the encryption key. The hashing algorithm MD5 was used as the encryption standard to generate the key for the application. The user's password and unique number were used as means for encryption to store the database of the chats. Various password guessing attacks were performed on this app and almost 40% of the passwords were successfully cracked. A number of methods were proposed to counter these attacks.

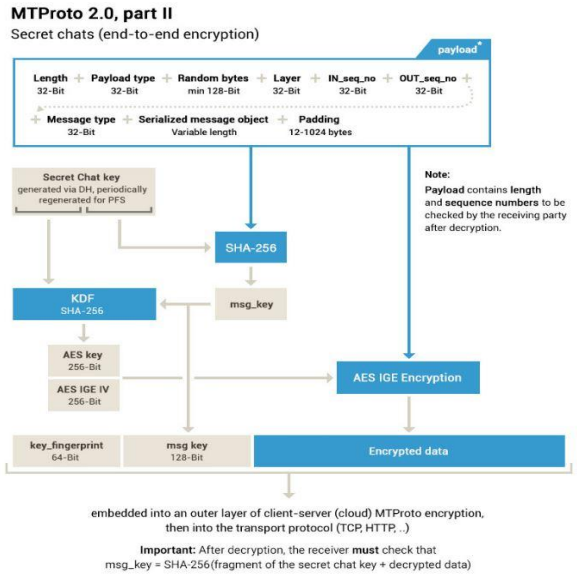


Telegram

Telegram is an instant messaging service application that was launched in 2013. It has 3 million users registering every day and 200 million active users. It was launched with a motive to provide high-end encryption. It also has a feature of self-destruction if the account is found to be not active. It offers a secret chat feature which enables the user to have end-to-end encryption. Through this feature, the chats are visible and restricted to the sender and receiver's mobile. The data is not stored on the servers and it can be self-destructed using timer. This feature avoids the man-in-the-middle attack and many such cryptographic attacks. This end-to-end feature is developed for the advance users which uses MTProto 2.0. This protocol uses the SHA-256 algorithm for encryption and number of padding bytes are involved in key generation. The Diffie-Hellman protocol is used for generating key for E2EE. The data is then encrypted with 256-bit AES, and an API call is made. Telegram server takes this request and ensures that the data is sent to the other party who is using secret chat. The key fingerprint is computed as follows:

- digest = md5(key + iv)
- fingerprint = substr(digest, 0, 4) XOR substr(digest, 4, 4)

The remote client is notified about the local layer of the sender and message is decrypted. This way it acknowledges the message and messages are successfully exchanged. Due to its high encryption standards, the data is sent without any cryptanalytics. This is the reason why most of the users prefer this messenger application over other messengers. The app immediately notifies with the updates whenever there is a change in these encryption standards.



III. RESULTS

It can be clearly stated that different messenger applications use their own techniques to secure the data of the user. In this paper, a detailed research was carried out to find the encryption algorithms used by different messenger applications. The results have been concluded in Table 1.

TABLE 1

S. No	Product Name	Encryption(s) Used	N-bit
1.	WhatsApp Messenger	AES-256, Curve25519	256 Bit
2.	Hike Messenger	AES-256(Web), RSA 2048 & AES-128 (Mobile App)	128 Bit & 256 Bit
3.	KakaoTalk	AES-128	128 Bit
4.	Telegram	AES-256	256 Bit

IV. CONCLUSION

It can be concluded that based on the priority of the features in the application, the most appropriate algorithm can be chosen. The speed and the time complexity for a given algorithm also matters when the features of the application are considered.

REFERENCES

1. Matthew Wangsadiredja, "Text and File Encryption Application for BlackBerry Using Cipher Feedback 8-bit Mode" in International Conference on Electrical Engineering and Informatics, 2011, pp 17-19
2. Komal D Patel, "Image Encryption Using Different Techniques" in International Journal of Emerging Technology and Advanced Engineering, 2011
3. Jusop Choi, "Forensic analysis of the backup database file in KakaoTalk messenger" in IEEE, 2017, pp 156-161
4. Md. Didarul Alam Chawdhury, "Security Enhancement of MD5 Hashed Passwords by Using the Unused Bits of TCP Header" in International Conference on Computer and Information Technology, 2008, pp 714-717

AUTHORS PROFILE

Maganti Manasa is a student currently pursuing final year in B.Tech, Computer Science from GITAM, Visakhapatnam. Her research interests are in the field of Cryptography, Machine Learning and Data Science.

Dasari Veera Reddy.Completed B.Tech and also M.Tech from Jayamukhi Institute of Technological Sciences, Warangal. Presently working in GITAM asAn Asst.Professor in the Department of Computer Science in Vizag location. His areas of interests are: Cryptography, CloudComputing, Artificial Intelligence and Internet of Things.
.

Amanapu Yaswanth,completed B.Tech from VITAM,,M.Tech from GITAM and Presently Pursuing Ph.D from GITAM (Deemed to be University).His Presently working as an Asst.Professor in the Department of Computer Science in GITAM.His Areas of Interest are Cyber Security and Software Engineering.

G.V.S Raj Kumaris presently working as Professor in Computer Science in GITAM. His Research Interests are Cryptography and Network Security.