IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

Secure SMS System for Android

[1*]Lalit Kumar Gupta, [2]Ananya Gupta, [3]Akshay Singh, [4]Abhishek Kumar

[1,2,3,4]Dept. of Computer Science Engineering, IET, Bundelkhand University, Jhansi, India

Corresponding Author - dr.lalitgupta.bu@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i3.179183 | Available online at: www.ijcseonline.org

Accepted: 13/Mar/2019, Published: 31/Mar/2019

Abstract- Communication (from Latin *communicare*, meaning "to share") is the act of conveying messages from one entity or group to another through the use of mutually understood signs. It not only facilitates the process of sharing information and knowledge, but and also helps people to develop relationships with others. Security matters to people differently. However, it is always required. Same is with our shared information. The main purpose of this paper is to introduce security of the text messages that people share among them. In this paper, we are presenting Secure SMS System for Android users, thus providing an End-to-End Encryption (E2EE). RSA algorithm of Cryptography and a Key generation algorithm have been used. Whenever a message is sent, it is not sent as a plain text; rather it is encrypted using the public key of the receiver to get the cipher text, which is transmitted to the receiver. At the receiver side, that cipher text is decrypted using the private key of the receiver, to get the plain text, the actual message that is sent to him. This would prevent the third parties from interfering into the text messages shared. This implementation can then be used by people in general as well as all the intelligence agencies.

Keywords- Cryptography, Encryption, Key, Cipher text**.**

I. INTRODUCTION

Communication is very necessary in order to socialize in the society. In the ancient times, when there was no internet and even electricity, people used to communicate among themselves via trained pigeons. This process was known as Pigeon Post. The pigeons flew as they were directed and the receiver got the letter that was actually sent for him.

Ages after, in 1930s the telephones were invented and people got connected through a better means. In the early 1980s, the cell phones were invented. These cell phones were portable and a certain amount of battery backup, that lasted for about 4 hours. In 1992, the first text message was sent- "MERRY CHRISTMAS".

These text messages are sent via the antennae in the phones. The antennas convert these text messages, either to binary codes or used dots and dashes to represent the text. These antennas sent this text to a few miles and to the tower. Fixed frequency radios waves help determine the tower that the message is sent by you. That tower then directs the message to the tower nearest the receiver and the receiver receives his message via his frequency radio waves.

Text messages were becoming popular day by day, due to the ease in their use. Gradually, people realized that the messages they were exchanging was not safe. SMS (Short Message Service) is a service provided by the telecom services, in order to increase the convenience of communication. The limit of standard SMS messages is limited to approximately 160 characters per message.

There are many existing applications in the play store available for free but they do not provide a security to our messaging. The messages could be accessed by the service providers and any third party that wants to go through your information. This was a big threat to the information exchanged by the people. A mechanism was needed to secure the information and messages of the people.

This way cryptography was introduced in messaging. Cryptography is a field of Network and Security, that sends the messages in a different form from what the actual message is, and only the authorized and authenticated receiver can access the real meaning of that message. The actual message that the user wants to send is called the plain text. The plain text when is altered, using an algorithm becomes the cipher text.

Changing the form of the text before sending it (plain text), so that none of the unauthenticated and unauthorized user can access it, using a specific algorithm is known as Encryption. Encryption is done the sender side, using a key.

When the cipher text is converted back to the plain text, at the receiver side using an algorithm is known as Decryption. Cryptography involves various keys that help in encrypting and decrypting the text. When the same key is involved while encrypting and decrypting the plain text and the cipher text, respectively it is called the Symmetric cryptography; otherwise it is called the Asymmetric cryptography.

Symmetric cryptography involves the concept of Key Distribution Centre (KDC). It is via KDC that the connection is established between the sender and the receiver for a certain amount of time. A key is generated by the KDC, when requested by the sender for communication with the receiver. That key has a time period for its validity [1].

Asymmetric cryptography involves two keys namely, public key and private key. A user has his public key as available for everyone, while the private key is kept secret with him. The plain text is encrypted using the public key of the user and then the cipher text is decrypted by the receiver using his private key [1].

End-to-end encryption (**E2EE**) is a system of communication where only the communicating users can read the messages. In principle, it prevents potential eavesdroppers – including telecom providers internet providers and even the provider of the communication service – from being able to access the cryptographic keys needed to decrypt the conversation [5].

The main purpose of this paper is to introduce security of the text messages that people share among them. In this paper, we are presenting Secure SMS System for Android users, thus providing an End-to-End Encryption (E2EE). RSA algorithm of Cryptography and a Key generation algorithm have been used.

Whenever a message is sent, it is not sent as a plain text; rather it is encrypted using the public key of the receiver to get the cipher text, which is transmitted to the receiver. At the receiver side, that cipher text is decrypted using the private key of the receiver, to get the plain text, the actual message that is sent to him. This would prevent the third parties from interfering into the text messages shared. This implementation can then be used by people in general as well as all the intelligence agencies.

II. LITERATURE REVIEW

SMS is a service provided by the telecom services, in order to increase the convenience of communication. The limit of standard SMS messages is limited to approximately 160 characters per message. There are many existing applications in the play store available for free but they do not provide security to us. The messages could be accessed by the service providers and any third party that wants to go through your information. This was a big threat to the information exchanged by the people. A mechanism was required to secure the information and privacy of the people.

Cryptography is also known as Cryptology. Cryptography can be defined as the process of converting a plain text into a cipher text or vice-versa, using certain keys and algorithms. The algorithms can be categorized as the Encryption and Decryption algorithms. Cryptography is used in order to increase the security of the shared messages and the data [2, 10].

In cryptography, plain text is the original message the sender wants to send to the receiver. The encryption algorithms are applied on the plain text, using different keys, in order to get the encrypted message. The actual meaning of the text is distorted in a way that it can be regained, so that no third party can get what the text is about. The resulting message is what is called the Cipher Text. The receiver reads this plain text, after it has been decrypted for him. In cryptography, cipher text is the text obtained after the plain text has been encrypted. It is the cipher text that is sent from the sender to the receiver. The cipher text may also be known as the encrypted text [7].

Encryption can be defined as a process of converting the plain text into cipher text. The actual meaning of the text is distorted in a way that it can be regained, so that no third party can get what the text is about. The cipher text may also be known as the encrypted text. The plain text is encrypted using a key [8, 9].

Decryption can be defined as a process of converting the cipher text into the plain text. In decryption, the actual meaning of the message is regained only when it has been transmitted to the receiver. The plain text obtained after decryption is known as the decrypted text. The cipher text is decrypted using a key [8, 9].

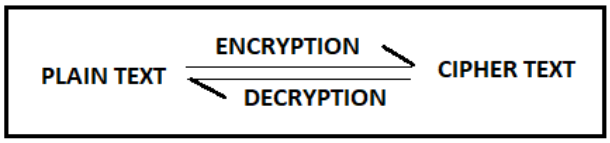

Figure 1. Cryptographic process

In symmetric cryptography, both the sender and receiver have a common key. The text is encrypted and decrypted using the same key. This key is valid only for a short time period. A centralized Key Distribution Centre provides keys to the sender and the receiver, when requested for a connection. AES (Advanced Encryption Standard) is a Symmetric Cryptography Algorithm. Symmetric

Cryptographic algorithms are also known as Private Key Cryptography.

In asymmetric cryptography, there are different keys for the encryption and the decryption of the text, unlike of symmetric cryptography. A single user has two keys- a public key and a private key. These keys are generated as the user registers him. His public key is available for everyone, i.e. it is public, whereas his private key remains with him. Asymmetric Cryptographic algorithms are also known as the Public Key Cryptography.

RSA, an asymmetric cryptographic algorithm was developed and introduced by Ron Rivest, Adi Shamir and Len Adleman in 1977. It is a Public key Cryptographic algorithm. There is no need to share a key privately between two communicating users because the public key is already shared using which the message is encrypted. RSA algorithm is based on the mathematical concept of product of two very large prime numbers, whose factorization is difficult task. A single user has two keys- a public key and a private key. These keys are generated as the user registers him. His public key is available for everyone, i.e. it is public, whereas his private key remains with him [3, 4]. We are using the RSA, asymmetric algorithm to the SMS System developed with Android Studio. Thereby providing a security to the messages, people share. The messages are sent as cipher text, encrypted by the public key of the receiver and will be decrypted using the private key of the receiver.

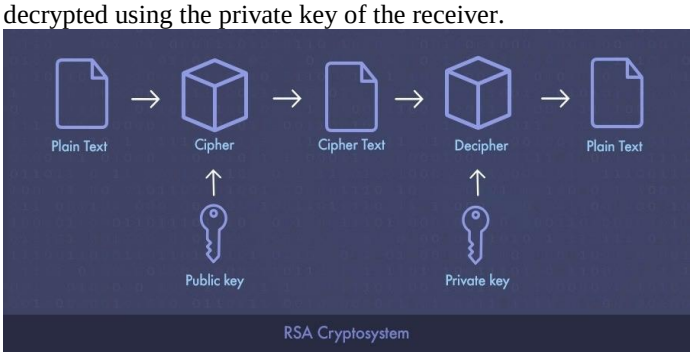

Figure 2. RSA Cryptosystem

III. HOW APPLICATION WORKS

We are developing a chat app via Android Studio and use End-to-End Encryption using the RSA algorithm of Asymmetric Cryptography. Thus, eradicating the threat to the security of the information shared, of the third party being able to access the private or official information. The chat app will have an activity for the registration of the user and then the login activity for all the registered users. After the registration of the user, with his name and his mobile number, two keys are generated- a public key and a private key. The public key of the user is visible to all the users in his contacts using the same application. The private key is kept secret with the user himself. The backend- the database will store the data of the users namely, their mobile numbers as the primary key, their respective passwords and the generated public and private keys. When the user wants to send a message, he will have to add the mobile number, along with his message, to which he wants to send that message. Whenever the user wants to view a message, he just needs to click on the message from the inbox. The decrypted message will appear.

MOBILE VIEW

- **Registration:** The user who downloads the application, will register him on the app, using his mobile number and name, and thus will generate a password for his login in the future.
- **Login:** A registered user can login anytime with his phone number and his password, in order to use the app.
- **Message:** Whenever the user wants to view a message, he just needs to click on the message from the inbox. The decrypted message will appear.
- **Send Message**: When the user wants to send a message, he will have to add the mobile number, along with his message, to which he wants to send that message.

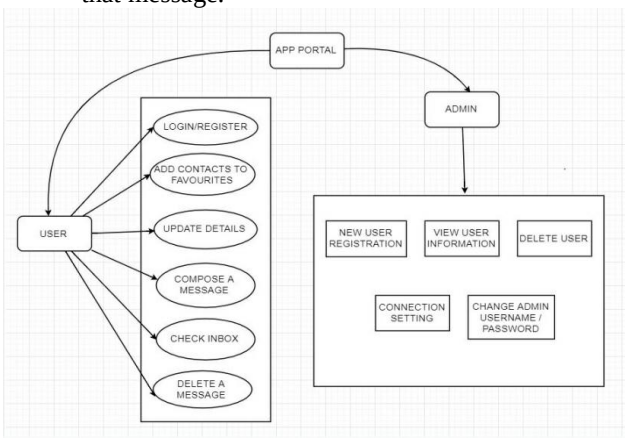

Figure 3. Implementation

IV. MODULES IN THE PROJECT

Modules are an essential part of any project. They define the functionality of the project in different parts. There will be four modules in the project. The modules will be:

1. SMS android application
2. Key generation
3. End-to-End Encryption

1. SMS ANDROID APPLICATION

The SMS app will be developed using Android Studio. As the user installs the app, he will register himself with his mobile number and create password for him. After that he can use the app anytime, simply by logging in.

REGISTRATION

- The user can register him with their mobile numbers and names.
- The user will generate their passwords and get registered.
- Using the RSA algorithm, the public and the private keys are generated.
- The public key of the user is visible to all the users in his contacts using the same application.
- The private key is kept secret with the user himself.

LOGIN

- The user can login himself with his registered mobile number and the password created by him at the time of registration.
- He is directed to the home page of the application.

INBOX

- A text editor will be available for typing the text message.
- When the user wants to send a message, he will have to add the mobile number, along with his message, to which he wants to send that message.

2. KEY GENERATION

Key generation algorithm is used to generate the keys- a public key and a private key, for the user when he will register on the app, with his mobile number. The algorithm can be described as follows:

- The key generation algorithm is the most complex part of RSA. The aim of the key generation algorithm is to generate both the public and the private RSA keys.
- Large Prime Number Generation: Two large prime numbers p and q need to be generated. These numbers are very large: At least 512 digits, but 1024 digits is considered safe.
- Modulus: From the two large numbers, a modulus n is generated by multiplying p and q.
- Totient: The totient of n,$\phi(n)$n,$\phi(n)$ is calculated.
- Public Key: A prime number is calculated from the range [3,$\phi(n)$)[3,$\phi(n)$) that has a greatest common divisor of 11 with $\phi(n)\phi(n)$.
- Private Key: Because the prime in step 4 has a gcd of 1 with $\phi(n)\phi(n)$, we are able to determine it's inverse with respect to mod$\phi(n)$mod$\phi(n)$.

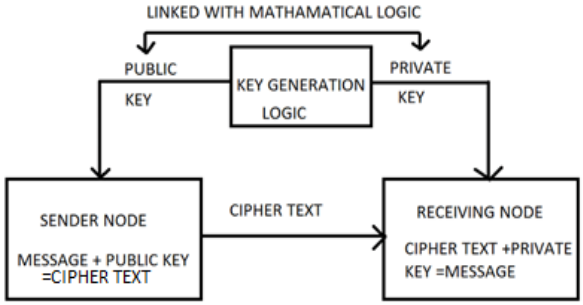

Figure 4. Key Generation

3. END-TO-END ENCRYPTION-

The messages are end-to-end encrypted using the RSA algorithm.

- The user types his message.
- The message is encrypted by the public key of the receiver.
- The message is sent to the receiver via telecom network.
- The message is received in the encrypted form.
- As the receiver opens the message he get the decrypted message.
- The message is decrypted by his private key.
- He can reply in the same encrypted way.
- This is the End-to-End Encryption.

V. TECHNOLOGIES USED

- FRONT END— ANDOID STUDIO AND JAVA
- BACK END— DATABASE—FIREBASE

The SMS system will be developed on the Android Studio containing activities for registration, login, inbox and create a new message.

The backend- the database will store the data of the users namely, their mobile numbers as the primary key, their respective passwords and the generated public and private keys.

VI. WORKING

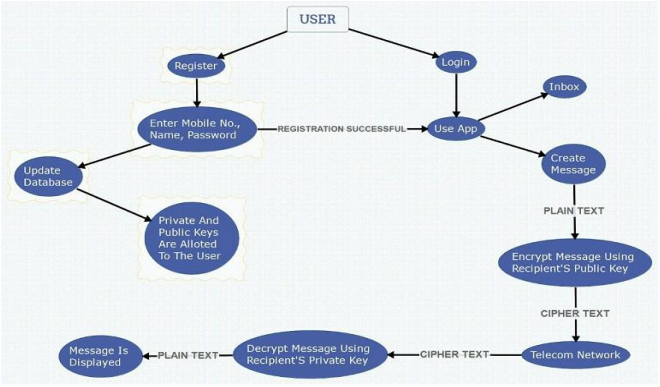

Figure 5. Flow Chart

- The user selects among the list of contacts those who are on the same platform (this app) he wants to send a message.
- A text editor is displayed to him.
- The user types his message.
- The message is encrypted by the public key of the receiver.
- The message is sent to the receiver via telecom network.
- The message is received in the encrypted form.
- As the receiver opens the message he gets the decrypted message.
- The message is decrypted by his private key.
- He can reply in the same encrypted way.
- This is the End-to-End Encryption.

VII. ADVANTAGES

- It is a password protected app.
- Only the messages that were sent encrypted are displayed.
- Reliability and security is offered.
- The user need not know the process of encryption and decryption.

VIII. CONCLUSION

In this paper we have presented an SMS app using Android Studio and used End-to-End Encryption using the RSA algorithm of Asymmetric Cryptography. Thus, eradicating the threat to the security of the information shared, of the third party being able to access the private or official information. The backend- the database will store the data of the users namely, their mobile numbers as the primary key, their respective passwords and the generated public and private keys. When the user sends a message to someone, the message is converted into the cipher text via the public key of the recipient. At the receiving side, the cipher text is decrypted into plain text via the private key of the receiver. In this way, any third party trying to get any information from the messages would fail in his motive and the information would be secured. This application can be used by intelligence agencies like RAW.

REFERENCES

[1] Delfs, Hans & Knebl, Helmut (2007). "Symmetric-key encryption". Introduction to cryptography: principles and applications.
[2] Hacker Lexicon: What Is End-to-End Encryption?".WIRED. 2014-11-25.
[3] RIVEST, Ronald L.; SHAMIR, Adi; ADLEMAN, Len. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM; 1978; 21.2: 120-126.
[4] Johnson, J.; Kaliski, B. (February 2003). "Public-Key Cryptography Standards (PKCS) : RSA Cryptography Specifications Version 2.1.
[5] RIVEST, Ronald L.; SHAMIR, Adi; ADLEMAN, Len. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM; 1978; 21.2: 120-126.
[6] William Stallings, Network Security Essentials Application and standards, 4th edition published by Prentice Hall.
[7] Van Tilborg, Henk C.A. (2000). Fundamentals of Cryptology.
[8] Bellare, Mihir. "Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements".
[9] Katz, Jon; Lindell, Y. (2007). Introduction to Modern Cryptography.
[10] Pelzl & Paar (2010). Understanding Cryptography. Berlin: Springer-Verlag.

Author Profile

Mr. Lalit Kumar Gupta pursed Bachelor of Technology from Purvanchal University, Jaunpur in 2001 and Ph.D. from Bundelkhand University in year 2016. He is currently working as Assistant Professor in Department of Computer Science & Engineering, Bundelkhand University, Jhansi since 2006. He is a member of various computer societies. He has published more than 10 research papers in reputed international journals. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Grid Computing, IoT and Computational Intelligence based education. He has 13 years of teaching experience.

