International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2019.3577

E-ISSN : 2454-6135

Volume.5, Issue 10
October -2019

Subject Review: SMS Encryption for Android Mobile using the Encryption Algorithm

Zainab Khyioon Abdalrdha[1], Farah Neamah Abbas[2] & Iman Hussein AL-Qinani[3]

[1,3] Teacher, [2]Assistant Teacher

[1-3] Department of Computer Science, Collage of Education, University of Mustansiriyah, Iraq

Abstract

Nowadays, SMS or messaging is a very common way of communication. So, it differs from the apps and instant messaging available but SMS is still one of the broad communication methods as it does not require internet connection and sending inexpensive, fast and modest SMS messages. When confidential information is replaced by SMS, it is difficult to protect information from secure SMS and ensure that the message is sent only by approved senders.

This research reviews and describes several methods used to encrypt SMS massage on android based on the encryption algorithm and compare these methods.

Key Words: *Short Message Service (SMS), Advanced Encryption Standard (AES), RC4, NTRU and Android.*

1. INTRODUCTION

Network security is a major problem in the world of wireless communications based on SMS or information sent between two people. At that time, there are many hackers to sensitive data of SMS and contact information. These unauthorized persons illegally infiltrate and access data from the network. Therefore, this is a big problem and needs security within the network. To solve these problems, provide security for SMS users use encryption techniques and algorithms and uses different keys to communicate. Private key, uses the public key for a secure and reliable message [1]. Short Message Service (SMS) is a form of communication of precise length, and SMS is used frequently. Therefore, SMS messages must be secured. There are different ways to secure SMS, one of them is encryption. Encryption has always been an important task. The main goal of all encryption activity is data security, the message is encrypted in this way, and can only be understood by the sender and receiver. The encryption algorithm is used to perform encryption and decryption [2]. Android is a free operating system and provides a platform and rich for developers from different quarters to create innovative applications with different programming interfaces such as application programming interfaces Android provides a complete platform for smart phone operators, developers and phone manufacturers to create innovative hardware and software services around the world [3]. In this paper, the benefits of SMS encryption in part 2. In part 3, we review the literature survey of SMS encryption in different cryptography, in part 4 we present the performance literature survey of the schemes discussed, finally, the conclusions about this review are made in part 5.

2. BENEFITS OF MESSAGE ENCRYPTION

Message encryption or SMS is now more popular in days. SMS was first used in December 1992, when well-known testing engineer Neil Bab Worth, 22, used the computer to send the text message "Merry Christmas" via Vodafone's GSM network to the phone of a person in the UK known as Richard Jarvis. Nowadays, businesses use many SMS for their business purposes. Therefore, it has become necessary to protect SMS messages in most businesses and customers [4]. To provide a secure communication between the sender and the recipient we need encrypted SMS. The security of any trading company is a concern such as banks that are responsible for mobile banking services. Additional encryption is required to secure SMS for business purposes to provide security for messages over the network [5].

3. LITERATURE SURVEY

In the last decade, there have been many studies and researches that have been examining methods of key generation because of its importance in the process of increasing security and in this part, we will review and discuss some research on this area.

In this paper, authors [6] Introduced Software Framework is SEE-SMS (Extensible and Effective SMS) This software is programmed in Java that allows the exchange of encrypted messages and the connection is secured according to the encryption of

the public key and is digitally signed. The keys were exchanged depending on the security protocol and this software used the ECIES and RSA encryption algorithms to encrypt communication channels. The identity and validity of the contacts involved in the communications were verified through signature systems; RSA, DSA and ECDSA were used. This program was able to validate the peer phone number using the framework. The plug-in was encrypted and added to SEESMS and devoted particular attention through the implementation of an effective framework in terms of implementation time and energy consumption.

In this paper authors [7] introduced a method running on the Android environment that encrypts messages before being sent by the user over the network allowing the encrypt messages before sending them over the network. The AES algorithm has been used to encrypt and decrypt data and this method can run on any mobile running the Android system environment.

In this paper Jongseok Choi and How on Kim [8] Due to problems related to SMS security, such as monitoring of user messages by national laboratories, two-way communication messages cannot be used because this will double the cost. So, he introduced the common public key encryption method to provide SMS security to solve the mentioned problems. SMS Gateway is used as an external tool for sending / receiving messages between mobile devices. That the attacker could not obtain the secret keys and private decryption in order to extract the normal message body.

Nenad Gligoric [9] Propose a solution using both compression and encryption for M2M connections via SMS, i.e. security work at the application layer thus providing security and reducing the size of data.

J. Bose and T. Arif [10] Used the gyroscope, acceleration sensor, and multiple positioning devices to encrypt SMS messages and the key will be in the form of gestures made by the user or can be sensor readings such as the site for example and the neural network was used to train the input gestures used as a key for the process of encryption and decryption The XOR method was used to encrypt data using gestures as the key. Finally, the app has been implemented on Android phones.

In this paper Asst. Prof. Dr. J. Stephan and Z.Dhaief, [11] This application is based on the RSA algorithm to encrypt a message and the length of 160 characters and after using the algorithm to encrypt the message in the Android environment is sent via the recipient's phone number by the sender and the application is programmed using the language of Java.

The authors in this paper, [12] used application is based on the AES algorithm to encrypt SMS message and sending a message encrypted in the Android environment over the network the application is programmed using the language of Java.

The authors in this paper [13] The researchers here presented the use of the NTRU algorithm, in the process of encrypting the messages of chat applications and because of the speed of encryption and decryption and given the importance of this topic, which requires high security to maintain the reliability and high speed of data sent.

The authors in this paper [14] View details Build an SMS security application framework that provides confidentiality, safety, authentication and non-repudiation of SMS. The framework hides from end users all the details related to certificate and key management. The main contribution is the use of short signatures to authenticate the origin of SMS messages, making it possible in a single package, 140 bytes SMS all the necessary information to authenticate the origin of encrypted messages, while still the user with a useful length of text.

B. PATIL in this paper [15] presented an idea about the process of exchanging encrypted and signed SMS messages. The public key is used encrypted and the key is exchanged via voice frame. And the application was written in .Net. The message is composed, encrypted and sent via an interface. On the side of the recipient's device, the message is first downloaded to the PC through the software package, the decryption applied to the message. The implementation of this application within the framework in terms of energy consumption and implementation time. This efficiency is obtained by implementing all available encryption systems in the framework using fully mature and improved encryption libraries and an empirical analysis was performed to determine which set of encryption systems and security parameters were able to provide a better trade-off in terms of speed / security and power consumption.

In this study H. Bodur and R. Kara [16] Used the RSA encryption algorithm to encrypt messages for secure messaging on the SMS channel that is validated on Android devices and the developer application is scanned. The feature and disadvantages of the application are shown and solution proposals are offered.

DOI : 10.31695/IJERAT.2019.3577

In this paper authors [17] introduced a message encryption method based on the AES 3D block encryption algorithm to provide a secure medium. Since the message is divided into a number of blocks where if the message size is more than 256 bits, it requires, additional time for the system to send the message, we will implement an SMS service that will reduce the time required while sending SMS.

In this paper M., K and A., Abidemi [18] introduced the application of AES algorithm to encrypt / decrypt messages and uses the same key in each side of the sender and recipient and the process of entering the key is entered by the user via mobile phone and this application was applied via Android phones.

In this paper Z. Abdalrdha [19] presents encrypted (SMS) message using (RSA) along with chaotic algorithm for encryption and data decryption to ensures safely and the provision of secrecy, authentication. This paper focuses on implementing an algorithm for SMS application on Android.

The authors in this paper [20] designed to encrypt SMS messages within the Android environment based on the AES algorithm (128-bit) to secure and encrypt data. The AES algorithm uses an encryption method that becomes difficult to penetrate by attackers and this application will allow the user to cipher and decrypt SMS messages (Short Message Service) safely and efficiently.

R. Rifki, A. Septiarini and H.Rahmania Hatta , in this paper [21] suggested in the application to encrypt messages based on the RC4 algorithm as being safe in sending SMS. However, RC4 includes the Key Scheduling Algorithm (KSA) and the Pseudo-random Generation (PRGA) algorithm. Accordingly, the RC4 algorithm has been updated with a random initial state so as to increase the randomness level of the main stream. The performance of the proposed method is evaluated based on coding and decoding time as well as the average correlation value. Based on the time, it indicates that the length of the sent SMS characters affects the encryption and decryption time, achieved the best correlation value of 0.00482.

In this paper [22] the authors are encrypted the message by strong cryptographic algorithms. It uses RSA algorithm for secure keys and AES algorithm to secure message. Authentication is implemented by using pattern lock. This system provides secure and reliable communication environment.

4. PERFORMANCE LITERATURES SURVEY OF THE SCHEMES:

In this section we will explain the performance analysis that will illustrate the behavior, performance and quality of services achieved by those algorithms or protocols. In this section we reviewed the performance of the algorithms used in the survey section. The table below contains the Ref-number, Algorithms, Working & Use of this algorithm, and Objectives of the review method of paper. This table is created after a paper review.

Table 1: Performance literatures survey Different Algorithms.

Ref-Number	*Algorithms or Techniques*	*Working & Use of This Algorithm*	*Objectives of This Work*
[6]	Rely on ECIES, RSA and DSA algorithms for channel encryption	• In the software (SEESMS), all encryption systems available in the frame pane are implemented using improved and mature encryption libraries. Second, an empirical analysis was carried out to determine which part of the encryption systems and security parameters they were able to provide the following specification: • Speed / security and power consumption are the best trade-offs.	• RSA and DSA algorithm keys of different sizes are used (512 to 3: 072 bit), and (112 to 256 bits for ECDSA) • Work on two mobile devices available for large scale measurement: Nokia N95 - 8GB specs (Symbian OS 9.2 - 332 MHz CPU) and HTC S620 have specs (Windows Mobile 5.0 - 201 MHz CPU).

DOI : 10.31695/IJERAT.2019.3577

[7]	Android Based on AES Algorithm	• The encryption key is 128-bit used in the AES algorithm. • Failure of statistical analysis and text encryption pattern due to the proposed algorithm components with strong deployment and confusion • The security feature of this algorithm and Altai considered more important is that there are no differential or linear attacks that can break this algorithm.	• Secure and improved SMS application. • Encrypted information from message recipients is preserved. • Decrypt message as requested by users. • Provide protection against misuse of message information by the user. • Improved security with high confidentiality of data.
[8]	A novel approach	• The method has three points: encryption process, SMS gateway and decryption process. • In the encryption process, the message is encrypted based on the public key that is derived from the shared public key , in SMS gateways all of the messages is know because The definitions of mobile devices stored in the server and all keys are created by definitions, in the decryption steps, the device can easily decrypt messages using its own key.	• Scheme design makes users communicate among themselves efficiently without sharing or sharing unique keys.
[9]	Signature using IMEI of device, key secret and payload is GZIP and encoding Base64	• To enable Unicode string transfer over 7-bit SMS the output is encrypted with Base64.	• The evaluation of the security mechanism applied in the GSM live network between two Android devices showed that the proposed secure communications have no effect on the time of SMS delivery compared to normal M2M calls via SMS. • It can provide better compression ratio.
[10]	sensors on the device is using to encrypted data stored and transmitted in mobile.	• Using touch gestures implemented encrypted SMS messages	• The encryption method used allows more secure encryption of data and then transfer over multiple channels.
[11]	Android Based on RSA Algorithm	• RSA using length of message is 160 character.	• Execution this method is faster in the mobile and added another layer of security. • This paper tested in different types of mobile types (GalaxyS3, Galaxy S4, HTC).
[12]	Android platform in AES algorithm in	• Analyzed the AES algorithm. There are total internal transformation (Sub Bytes, Shift Rows, Mixed Column and ADD Round Key). • Android platform, a package javax. crypto. chiper is called to make it easier in performing the coding.	• The different of testing are performed on applications are: • Compatibility testing and Interface testing. • Se Low level resource testing. • services testing and Performance testing. • Operational testing, Installation tests and Security Testing. • GUI (Graphical User Interface) and Emulators.
[13]	Android platform in NTRU Algorithm	• Key size of NTRU is Very small. • Key Generation of NTRU is 200 times. • Encryption of operation /sec of NTRU is 1113 times. • Decryption/sec of NTRU is 1132 /ms for NTRU-251.	• Less execution times. • Decrease decoding time. • Output factor productivity to be less useful in the consumption of the mixture

DOI : 10.31695/IJERAT.2019.3577

		• NTRU account strength is lower when compared to both mobile and smart cards. • Speed of NTRU is Faster. • Efficiency of NTRU is Fastest.	
[14]	ECIES or RSA-OAEP	• This application can be used for secure transportation. • Use authenticated and authentic encryption and short digital signatures that make gathering all the information in a text message essential for encrypted SMS authentication, while maintaining a useful length of messages.	• Flexible trade-offs between security and message length provide three levels of security: (1) confidentiality only, (2) confidentiality and message authentication, and (3) confidentiality, origin authentication and non-repudiation. • Providing easy-to-use security levels and seamless encryption integration are addressing the usability of security features.
[15]	Android platform in RC4 and AES with Rijndael encryption engine. This paper simulation operation in paper [6].	• Using RC4 and AES in Secure SMS Management Center includes two components: 1- The components and structure of the SEESMS program include the following modules: • • Registration service (RS) • Server Message Handler (SMH) • Secure Storage (SS) • Cryptosystem Engines (CE): 2- To exchange digitally signed and encrypted SMS. It includes the following parts. • Message Handler (MH) • Secure Storage (SS) • Cryptosystem Engines • Keys Communicator	• CE are modules that secure messages that are exchanged with a remote user and each CE carries an encryption system and provides three standard functions: generation of key, message plaintext / cipher and message signing / verification. • Keys Communicator is the unit responsible for implementing the client's key exchange protocol, used to deliver client-generated encryption keys to SSMC. • Analysis of the results clearly shows that Rijndael has better encryption strength while RC4 provides better energy conservation.
[16]	Android platform in RSA encryption algorithm	• RSA public key cryptographic algorithm is one of the most reliable algorithms of private key encryption algorithms for SMS encryption.	• This method has been tested for messages in different sizes of keys and in terms of power and key speed. • When the key is created, different keys can be used for the key that is created for operations and changes are reported in encrypted messages. • In this way the encryption process is used in secure messaging
[17]	Use the 3D-AES block encryption algorithm depending on the Android platform.	• The SMS is encrypted and Send this encrypted message and secrete key to the receiver through GSM. • GSM is used for routing the calls • Receiver received this encrypted message and the secrete key. Decrypt this message. Receiver receive the plaintext message.	• SMS is a simple, straightforward and easy to use. • The importance of this method is to protect encrypted data against various attacks. • Its application can be used for secure data transfer without any damaged data segment.
[18]	Android platform in AES (Advance Encryption System)	• The same encryption key is also used to decrypt the encrypted binary file. • This research work has a lot of benefits to both private and public firm and even individuals to protect their confidential information on mobile phones.	• This research does not require SMS gateway for the message to be sent from the sender to the receiver

DOI : 10.31695/IJERAT.2019.3577

[19]	RSA & chaotic Algorithm	• RSA is strong encryption but the secret increment when using chaotic algorithm is a well method for encryption message, the combination of chaotic theory and cryptography forms an important field of information security	• Implemented in mobile environment with android operating system • the method was tested in various types of operators (such as the S3, Galaxy S7, Galaxy j7, Huawei Nova2 plus, HTC)
[20]	Android platform in AES 128 -bit algorithm	• This method is a performance evaluation for the encryption of the three-block message • The method used for encryption over the GSM network provides secure transmission of confidential data.	• The app has been tested on buildings with an Android operating system with the following specifications: Version 4.1 (Jelly Bean), the mobile phone has a Cortex-A5 processor running at 1 GHz and 4 GB internal memory and 786 MB RAM. • • 100 random series of short messages were selected to evaluate performance • The proposed scheme for the work of this application on a phone showed the result that it is convenient and easy to implement
[21]	RC4 with random initial status in the Android platform	• Encrypt and decrypt SMS in this application	• Evaluate this method using 225 of data. • The results of the evaluation showed that the method is affected by the number of letters and the number of SMS messages, the specifications of the phone and the key used • The correlation value is affected only by the number of characters in the SMS message and the key, its key value in this application is (0.10188) showing more improvement compared to the Vigenere method (0.81229) and Play fair (0.21345).
[22]	RSA algorithm for secure keys and AES algorithm for the encryption message	• This application has been used in mobile phones running on the Android environment to encrypt SMS messages	• During the tests the results showed according to the proposed scheme that it is convenient and easy to implement on the mobile device

5. CONCLUSION

In this paper, we reviewed a different SMS encryption technique based on Android during the period (2010-2019). We discussed security, text encryption, and types of SMS software for mobile phones and a review of the paper literature survey of some authors. The methods are compatible with any types of mobile phones using Android. Our future work is to review and review the paper literature survey to encrypt SMS text messages in Android and compare it with the traditional encryption system. When reviewing the proposed research on message encryption in several types, we noticed the efficiency and security of the algorithms used in all types of mobile devices that support JAVA and are compatible with mobile phones and tablets that

DOI : 10.31695/IJERAT.2019.3577

support the Android environment. This review of the paper literature survey also provides a brief description and analysis of algorithms, and provides some assistance in improving encryption systems to ensure network security.

ACKNOWLEDGMENT

The authors would like to thank AL_Mustansiriyah University (www.uomusiriyah.edu.iq), Baghdad-Iraq for its support in the present work.

REFERENCES

[1] Hassinen M., "Java based Public Key infrastructure for SMS Messaging", IEEE, ICTTA, pp. 88-93, 2006.

[2] Nishika and Rahul Kumar Yadav, "Cryptography on Android Message Applications – A Review" International Journal on Computer Science and Engineering (IJCSE), ISSN 0975- 3397, Volume 5, No. 05, pp. 362-367,2013.

[3] Bimal Gadhavi and Khushbu Shah, "Analysis of the Emerging Android Market" Project Report Presented to SanJosé State University May 2010.

[4] Muhammad Waseem Khan, "SMS Security in mobile devices", International Journal Advanced Networking and Application,Volume 5,Issue 2,pp. 1873-1882,2013.

[5 Md. Asif Hossain1, Sarwar Jahan, M. M. Hussain, M.R. Amin, S. H. Shah Newaz "A Proposal for Enhancing The Security System of Short Message Service in GSM 2nd International Conference on Anti-Counterfeiting, Security and Identification. doi:10.1109/iwasid.2008.4688386 ,2008.

[6] De Santis and A. Castiglione, "An Extensible Framework for Efficient Secure SMS" IEEE Computer Society Washington, DC,USA,ISBN 978-0-6695-3967, Volume 6, pp. 843-850,2010.

[7] Rohan Rayarikar, Sanket Upadhyay and Priyanka Pimpale," SMS Encryption using AES Algorithm on Android", International Journal of Computer Applications, Volume 50– No.19, pp. 0975 – 8887, July 2012.

[8] J. Choi and H. Kim," A Novel Approach for SMS Security", International Journal of Security and Its Applications, vol. 6, pp. 373-378, 2012.

[9] N. Gligoric, T. Dimcic, D. Drajic, S. Krco, and N. Chu, "Application-layer security mechanism for M2M communication over SMS", Proc. Telecommunications Forum (TELFOR), 2012, 5-8.

[10] J. Bose and T. Arif," Encryption in mobile devices using sensors, Proc. Sensors Applications Symposium (SAS)", IEEE, 2013, 55-60.

[11] Asst. Prof. Dr. Jane J. Stephan and Zahra Salah Dhaief," SMS Encryption by Using Android Operating System", Iraqi Commission for Computers & Informatics (ICCI), Iraqi Journal for Computers and Informatics (IJCI) Vol (1) Issue (1), 2014.

[12] Jayeeta Majumder, Sagarjit Das and Sayak Maity "SMS Encryption in Android Platform", International Journal of Computer Engineering and Applications, Volume IX, Issue V, May 2015.

[13] Er.Amanpreet Kaur and Er. Navpreet Singh, "SMS Encryption using NTRU Algorithm" International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015) 96 Vol. 3, Issue 2 (Apr. - Jun. 2015).

[14] Alexandre Melo Braga, Romulo Zanco Neto, André Luiz Vannucci1 and Ricardo Shiguemi Hiramatsu" Implementation Issues in the Construction of an Application Framework for Secure SMS Messages on Android Smartphones", The Ninth International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2015.

[15] Bhimrao Patil, "SMS Security Using RC4 & AES" Indian J.Sci.Res. 11 (1): 034-038, 2015.

[16] Hüseyin Bodur and Resul Kara, "Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application" H. BODUR et al./ ISITES2015 Valencia –Spain.

DOI : 10.31695/IJERAT.2019.3577

[17] Varsha S. Bari,Nileema R. Ghuge,Chaitali C. Wagh,Sayali R. Sonawane and Mr.M.B. Gawali "SMS Encryption On Android Message Application" Vol-2 Issue-2 2016 , IJARIIE-ISSN (O)-2395-4396

[18] Murtala, Kabir and Adeniyi, Abidemi," Message Encryption and Decryption on Mobile Phones", Tetfund Sponsored Kwara State Polytechnic Journal of Research and Development Studies Vol. 5. No. 1 June 2017.

[19] Zainab khyioon Abdalrdha, "SMS Encryption of Android Mobile by Using RSA and Chaotic Algorithms", Volume 4, Issue 12, Publication Date: 18/12/2017. DOI: 10.21884/IJMTER.2017.4381.VCVNU.

[20] Muhammad Noman Riaz and Adeel Ikram "Development of a Secure SMS Application using Advanced Encryption Standard (AES) on Android Platform", I.J. Mathematical Sciences and Computing, 2018, 2, 34-48 ,Published Online April 2018 in MECS (http://www.mecs-press.net) DOI: 10.5815/ijmsc.2018.02.04.

[21] Rifki Rifki, Anindita Septiarini and Heliza Rahmania Hatta "Cryptography using Random Rc4 Stream Cipher on SMS for Android-Based Smartphones", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 12, 2018.

[22] Jitha P V and Unnikrishnan S Kumar, "SMS Security System Using Encryption Techniques", Jitha P V et al, International Journal of Computer Science and Mobile Computing, Vol.8 Issue.5, pp. 132-142, May- 2019.

DOI : 10.31695/IJERAT.2019.3577