SMS ENCRYPTION OF ANDROID MOBILE BY USING RSA AND CHAOTIC ALGORITHMS

Zainabkhyioon Abdalrdha

1Al-Mustansiriyah University, College of Education Department of Computer Science

Abstract - At present, SMS or messages are a very common way of communication. So it's different from the applications and instant messaging available but SMS is still one of the widespread ways of communication because it does not require an Internet connection and send SMS messages are inexpensive, fast and modest. When secret information is replacement using SMS, it so hard to protect information from SMS safe and it ensures that the message is sent only by authorized senders. This research describes a solution which provides (SMS) safely and ensures the provision of secrecy, authentication. We have used the public-key cryptosystems (RSA) along with chaotic algorithm for encryption and data decryption. RSA also provides 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. This method was implemented in mobile environment with android operating system. The system was implemented using the JAVA language and the proposed method was tested in various types of operators (such as the S3, Galaxy S7, Galaxy j7, Huawei Nova2 plus, HTC).

Keywords - Advantages of Message Encryption, RSA and Chaotic Algorithms, and Android Architecture

I. INTRODUCTION

Many organizations use SMS tools to communicate. It therefore requires strong security around SMS using encryption as well as decoding techniques [1].

SMS security or information is an important problem in network secure connectivity. Encryption and decryption algorithms are used by many authors to evaluate performance and safety. The algorithm Progress better performance but need more time to encryption [2]. The users who use the RSA and chaotic algorithms in encryption and decryption massage. In this paper, we discuss the advantages in using SMS encryption. In part 2, we review overview of RSA and chaotic algorithms. In part 3, we show the programming platform for mobile phones. In part 4, we show General Structure of the Proposed Approach and General Algorithm of the Proposed Approach. In part 5, we show execution of the proposed system, some conclusions about this review are done in part 6.

A. Advantages of Message Encryption

Encryption or (Short Message Service) SMS service is now more generally these days. Encryption or SMS service is first used in December 1992, by using Neil Papurt, a 22-year-old test engineer, to send text message "Happy Birthday" via the Vodafone GSM network to Richard Jarvis phone in the UK. In many companies the use of SMS was provided for their purposes. Security SMS’s has become more specialized for business organizations and clients [3]. There is a need for end encryption in order to provide meaningful security communications. Security is a major concern for any trading company like banks that will provide these services over the cellular telephone. Today also there is no such plan that provides secure SMS. Moving SMS in a network is not safe at all. Therefore, we use encryption to secure SMS for commercial purposes [4]. Encryption of message is a text format for accurate connection length. SMS messages are frequently used. SMS is used very frequently so you must

DOI:10.21884/IJMTER.2017.4381.VCVNU
secure it and encryption it. Encryption was always an essential assignment. The main purpose of all encryption work is to maintain data security. When you encrypt messages, only the sender and the recipient of the messages is understood. The encryption algorithm is used to make encryption and decrypt code[5].

B. Overview of RSA and Chaotic Algorithms
In this part will explain RSA and Chaotic Algorithms

1. RSA Encryption and Decryption
   RSA algorithm is an algorithm that has been used for the modern computer used to encrypt messages and decryption. The RSA algorithm is a public encryption algorithm that uses two general keys and the other one. RSA stands for Ron Rivest, Adi Shamir, and Leonard Adleman, who was first described publicly in 1978. RSA algorithm is an asymmetric encryption system that uses two sets of keys to encrypt and decrypt messages to ensure quality information security. In its performance, the keys are generated through a process of complex mathematical computation. The two keys are generated for encryption is public and private keys. The public key is distributed to the sender of a message to encrypt the message whiles the receiver of a message keeps the private key secretly to decrypt the public key encrypted message.
   The steps below are the processes in generating public and private keys using RSA
   1. Choose two large prime numbers k, l, and k! = l;
   2. Calculate q = k * l;
   3. Calculate A (q) = (k-1) * (l-1),
   4. Choose e, as well as gcd(e, A (q)) = 1.1 <e <A (q);
   5. Is calculated d, as well as d * e Mood A (q) = 1, i.e. d is the inverse of Multiplicative e in Mode A (q);
   6. Get the public key it is Ku = {e, q};
   7. Get the private key it is Kr = {d, q};

   In 1978, the paper was published by R. Revist, A. Shamir, and L. Adelman. In this paper, it describes the public key cryptography system, including key generation and public key, whose security depends on the supposed difficulty of calculating integers in key factors. This encryption, which became known as abbreviation of author's names, stood as an encryption and stood the test of time to the present day, where it is used in banking encryption applications of banking, e-mail security and e-commerce on the global network [6].
   Many applications are used for RSA algorithm but in the practical side it is often used for [7]:
   • Encrypt a small portion from data, especially for main transport
   • Digital signatures, in order to obtain digital certificates on the Internet.

2. Chaotic Algorithm:
   Chaotic cryptology includes two integral opposite parts: Chaotic cryptography and chaotic cryptanalysis. Chaotic cryptography is an application of mathematical chaos theory to practice encryption, study or techniques used to convey information in particular and secure with a third party or opponent. It has long sought to use chaos or randomization in encryption by entities that want a new method to encrypt messages. However, because of the lack of accurate security features can be proven and low appropriate performance, chaotic encryption has encountered setbacks.
   The encryption algorithm and decryption based on the chaos [8,9] The chaotic algorithm method is an efficient method and deals with the problem of data transfer speed which is a very safe method. In recent times there have been many researches on the method of chaotic encryption system which has a number of important characteristics, such as reliance on initial conditions and system identifiers, pseudo-properties, periodicity, topographic tension, etc. Most characteristics meet certain requirements
such as diffusion and mixing sense of encryption. Therefore, chaotic encryption system has more practical applications. One-dimensional chaos systems with advantages that are characterized by its high-level efficiency and simplicity, such as the logistics map, have been widely used now.

The text before the cryptography is called by the plain text which is the message that is entered by the sender, and the message to be encrypted is called text codes, which is referred to here as P and C, respectively. The encryption operation of the code can be described as $C = E_k(P)$, where $K_e$ is key of encryption and $E(.)$ is function of encryption. Similarly, the decryption procedure is $P = D_{k_d}(C)$, where $K_d$ is the key decryption and $D(.)$ is function of decryption. When $K_e = K_d$, the cipher is called a symmetric cipher. For private key ciphers, the encryption key and the decryption key $(K_e, K_d)$, where the public key is published and your private key is kept confidential and there is no need for extra secret channels to transfer the key [10].

C. Platform of programming for mobile  
1. AndroidSystem

Android operating system is one of the most famous terms today in the world of mobile. People have resorted to Android phones and applications because of the creation of secure websites among users. An android is software for mobile devices based on the Linux kernel and was founded in 2003 by Andy Rubin a number of other workers in Palo Anto California, operating system that contain operating system, middleware and key applications [11]. Android is a free operating system with rapid growing mobile platforms. It also provides rich and fast platforms for third-party developers to build applications with aggregates available for Application Programming Interfaces (APIs). The Android operating system provides an integrated platform for the work of the wizards and the development of a problem solving mechanism to create a global class in terms of the software and services it provides [11].

2. Architecture for Android System

Android operating system can be classified into five main layers: application, application framework, libraries, Android runtime and Linux kernel. There are a number of components that make
up the Android application as shown in block diagram in Figure 2: android operating systems architecture.

- The Applications part is the highest layer in the android system architecture. This part represents the basic applications that can be found for devices that are represented such as telephone calls, email client, SMS program, calendars, browsers, and others. That is written in Java language and other languages [12].

- Application Framework is a layer higher than the system structure. It is the framework or the way the developer follows it through application development. The developer fully accesses the same framework as used by the previous layer [12, 13].

- Libraries area layer containing software libraries written in Java for the development of Android applications. A different of libraries, from surface manager to libc, are written in different languages and these libraries are available for developer to be used through the framework application [14].

- Android Runtime is the fourth layer in android system architecture. This layer contains the so-called Dalvik Virtual Machine which is a type of JVM has been improved and modified to suit the Android system [14].

- Linux kernel is a layer at the bottom of the structure which is responsible for handling its own hardware. Android relies on Linux for basic system services such as memory management, power management software and a number of other services [15].

![Android Operating Systems Architecture](image)

**Figure 2. Android Operating Systems Architecture [16].**

**D. General Structure of the Suggested Approach**

The proposed Approach attempts to improve security of information that is encryption SMS. The general design of the proposed Approach illustrated using the general algorithm shown in figure (5). The general design of the encryption process of suggested method illustrated using the flowchart offered in figure (3). The general design of the decryption process of the suggested method illustrated using the flowchart offered in figure (4).
Figure 3. Flowchart Encryption of the Proposed Approach

Figure 4. Flowchart Decryption of the Proposed Approach
1. The General Algorithm of the Suggested Method

This part illustrates the main algorithm of the proposed method. It is offered in Figure (5).

| **Input:** | SMS (plain text) |
|------------|------------------|
| **Output:** | Cipher text      |

- **Step1:** Enter the message
- **Step2:** Encode SMS by using the RSA algorithm
- **Step3:** The result is cipher text also encrypted using chaotic algorithm
- **Step4:** Send the SMS to receiver message.
- **Step5:** SMS receiver applies proposed approach to decryption of the SMS.
- **Step6:** The decryption process was performed using the RSA and chaotic algorithm to decrypt SMS.
- **Step7:** The result of the decode is plaintext
- **Step8:** End.

![Figure 5. Main Algorithm of the Suggested Method](image)

II. THE EXECUTION OF THE PROPOSED APPROACH

Each step in main algorithm (5) will be illustrated in the following example. Here we will present the main interface of the suggested method, which is two parts of (encryption and decryption), shown in figure (6).

![Figure 6. The Main Interface of the Suggested Method](image)
Step1: Click on the window encryption operation to view the encryption algorithms used in this search offered in Figure (7).

Step2: Enter the SMS “well come” as illustrated in Figure (8).

Figure 7. Window encryption
Figure 8. SMS is Enter
Step 3: SMS is “well come” using RSA algorithm, the result is Cipher text and it is then encoded using the chaotic algorithm as illustrated in Figure (9) and Figure (10).

Step 4: After access the SMS for receiver will work to apply decryption operation by take copy of the SMS from message of mobile that result from chaotic algorithm then click back to decryption process, as illustrated in Figure (11).
Step 5: Paste the cipher text from chaotic algorithm then click on the decryption chaotic algorithm, then choice RSA algorithm to extract plain text as shown in Figure (12) & Figure (13).

**Figure 12 Decryption of Cipher text using Chaotic Algorithm**

**Figure 13. Decryption Cipher text using RSA algorithm**

**Step 6:** The result of the decryption is plaintext.
**Step 7:** End.

**III. CONCLUSIONS**

1. In this paper, we will discuss about the security of the relay SMS in mobile and how to encrypt and decrypt them, programming platforms of all kinds for the mobile phones and RSA and Chaotic
Algorithm, and This approach presents a method for encryption SMS messages of mobile in the android operating system environment.

2. We concluded that it is difficult to decrypt the message when it is encrypted twice using the RSA algorithm and once using the chaotic algorithm, the proposed method will be more secure.

3. Since data transmission through mobile is largely used nowadays, it is rarely focused on the issue of integrity and confidentiality of received data. Our main objective in this is to demonstrate how data can be encrypted. This scheme is particularly applied in using RSA and Chaotic algorithms together.

4. This application provides a secure, fast, and strong encryption of the data.

5. The system was implemented using the JAVA language and the proposed method was tested in various types of operators (such as the S3, Galaxy S7, Galaxy j7, Huawei Nova2 plus, HTC).

6. In future work we will use the NTRU algorithm and chaotic algorithm to encryption and decryption SMS and implement from through mobile and Compared with traditional encryption in terms of time and speed in encryption and decryption operations for testing purposes.

VI. ACKNOWLEDGMENT

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

REFERENCES

[1] M.Agoyi, D.Seral, “SMS Security: An asymmetric encryption approach “, IEEE, Internat. Conf. on Wireless Mob.Comm., pp.448-452,2010

[2] Sunita B. , Anita B., S.K.Sharma “ A new Approach towards Encryption Schemes: Byte Rotation Encryption Algorithm", World CECS 2012.

[3] Muhammad Wassem Khan, “SMS Security in mobile devices” ,International Journal Advanced Networking and Application, Volume 5, Issue 2, pp 1873-1882,2013.

[4] 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.

[5] 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

[6] Richard A. Mollin, “Codes: The Guide to Secrecy from Ancient to Modern Times”, ISBN 978-3-642-04100-6, Springer, 2010.

[7] Huang Yuanshi, XuRongcong, Lin Weiqiang, “An Algorithm for JPEG Compressing with Chaotic Encrypting”, Proceedings of the International Conference on Computer Graphics, Imaging and Visualisation (CGIV’06), 2006

[8] PengFei, Shui-Sheng Qui, Long Min, “An Image Encryption Algorithm based on Mixed Chaotic Dynamic Systems and External Keys”, Proceedings of 2005 International Conference on Communications, Circuits and Systems,.Vol. 2, pp.1139, 27-30 May 2005.

[9] M.SuryaBhupal Rao1, Dr.V.S.GiridharAkula2"CHAOTIC ALGORITHMS USED FOR ENCRYPTION AND DECRYPTION ON MOVING IMAGES",ISSN 2320 – 2602, Volume 2, No.8, August 2013.

[10] BimalGadhavi and Khushbu Shah, “Analysis of the Emerging Android Market” Project Report Presented to SanJosé State University May 2010.

[11] Jianye Liu, “ Research on Development of Android Applications” Fourth International Conference on Intelligent Networks and Intelligent Systems , IEEE 978-0-7695-4543-1,Volume 3,pp 69-72,2011

[12] Chao Wang, Wei Duan, Jianzhang Ma and Chenhuri Wang, “The research of Android System architecture and application programming” Computer Science and Network Technology International Conference (ICCSNT),Volume 2 , pp 785 – 790,2011.

[13] Huang, Qing: An extension to the Android access control framework, 2011

[14] Vaibhav Kumar Sarkania, “ Android Internals” International Journal of Advanced Research in Computer Science and Software Engineering, ISSN 2277 128X, Volume 3, Issue6, pp 143-147,2013.

[15] Er.Amanpreet Kaur1, Er. Navpreet Singh2,"SMS Encryption using NTRU Algorithm",ISSN : 2347 - 8446 (Online), Vol. 3, Issue 2 ,Apr. - Jun. 2015.