SMS Encryption by Using Android Operating System

Asst. Prof. Dr. Jane J. Stephan[1], Zahra Salah Dhaief[2]

[1]Iraqi Commission for Computers and Informatics/ Baghdad, Iraq

E-mail: janejaleel@yahoo.com

[2]Computer Science Department,University of Mustansiriyah/ Baghdad, Iraq

E-mail: zehraa_84@yahoo.com

Abstract: Mobile phones are the most commonly used devices in today's scenario. The expanding use of mobile phones, telecommunication companies added feature such as SMS (Short Messaging Service) in order to attract more customers. The Short Messaging Service (SMS) has become very popular for sending messages containing information among mobile users. Alongside, the need for the secure communication became more imperative. SMS security ensures security of messages from the access of unauthorized users. Using RSA algorithm to encryption of message that length is 160 character. In this paper present approach encryption message for type a SMS then send to other user. This approach is applied in mobile environment with android operating system. The platform used here is JAVA and the proposed approach is tested different types of mobile types (Galaxy S3, Galaxy S4, HTC).

Keyword: Cryptography, RSA Algorithm, Android Operating System, Short Messaging Service (SMS).

الخلاصة: ان الهاتف يعتبر من الأدواتَ الاكثر استعمالا في سيناريو اليومِ. ان الاستعمال الواسع للهواتف النقالة جعل من شركات الاتصال اضافة خدمة الرسائل القصيرة (SMS) لجذب اكثر عدد من المستخدمين. خدمة الرسائل القصيرةِ (SMS) أَصْبَحتْ اكثر شعبيةَ لإرسال الرسائلِ التي تَحتوي معلومات مهمة بين مستخدمو الهواتف النقّالةِ، حيث اصبحت الحاجة للإتصالِ الآمنِ اكثر أولويةَ. الكتابة المشفَّرة تعتبر من التقنيات الموثوقةِ لاخفاء المعلوماتِ. سرية (SMS) لضمان السرية للرسائل من وصول الاطراف غير مخولة، استخدام خوارزمية RSA لتشفير الرسالة التي طولها هو ١٦٠ حرف ليتم تشفيرِ الرسائل من نوع (SMS) ثمّ تُرسلُ إلى المستلم الآخرِ. وقد تم تطبيق هذة النظرية في بيئةِ الهاتف النقّال للنظامُ تشغيل الاندرويد. وتم إستعملَ برنامج جافا كلغة برمجية و تم اختبار النظرية المُقتَرَحَة في انوعِ مختلفِة للهاتف النقّال من نوع (Galaxy S3, Galaxy S4, HTC).

1. Introduction

The computer has been in constant evolution since the middle of the 20th century. Computers are continued to get smaller in size, using less power and performing more advanced calculations. In 2007 Apple released their iPhone to achieve the next goal in computing. This new type of communication tool, called Smartphone, is generally referred to as a phone. A Smartphone is a handheld computer, which can place phone calls. One competitor to Apple iPhone OS is the Android OS.

Android originates from a small software company [1]. The main motive of using Mobile phones has been the exchange of information between two users. The Short Messaging System was introduced with GSM mobile phones and it is very rapidly become popular among users [2].

2. Cryptography

Cryptography is the art or science of keeping secrets. . Cryptography is about secure communication through insecure channels. The idea of a cipher system is to disguise confidential information in such a way that its meaning is unintelligible to an unauthorized person [3]. The information to be concealed and the operation of disguising it is known as **encryption**. The encrypted plaintext is called the **cipher text** or **cryptogram** and the set of rules used to encrypt information plaintext is the **encryption algorithm**. Normally the operation of this algorithm depends on an **encryption key**, which is input to the algorithm together with the message. In order that the recipient can obtain the message from the cryptogram there has to be a **decryption algorithm** which, when used with the appropriate **decryption key**, reproduces the plaintext from the cipher text [4]. The cipher system is shown in figure (1)

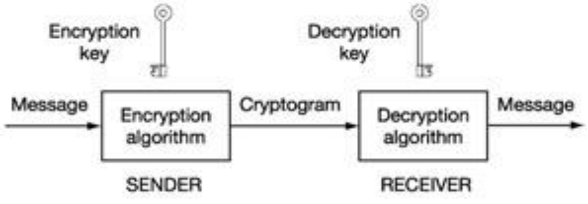


Figure 1: Cipher system

Encryption is the most effective way to achieve data security. The process of Encryption hides the contents of a message in a way that the original information is recovered only through a decryption process [5]. The purpose of Encryption is to prevent unauthorized parties from viewing or modifying the data. Encryption occurs when the data is passed through some substitute technique, shifting technique, table references or mathematical operations. All those processes generate a different form of that data. The unencrypted data is referred to as the plaintext and the encrypted data as the cipher text, which is representation of the original data in a difference form. Key-based algorithms use an Encryption key to encrypt the message. There are two general categories for key-based Encryption: Symmetric Encryption which uses a single key to encrypt and decrypt the message and Asymmetric Encryption which uses two different keys a public key to encrypt the message, and a private key to decrypt it [6]. In this paper RSA algorithm is used to encrypt the message from type public key encryption. It was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978. The Rivest-Shamir-Adleman (RSA) scheme has since that time reigned supreme as the most widely accepted and implemented general-purpose approach to public-key encryption. The RSA scheme is a block cipher in which the plaintext and cipher text are integers between 0 and n- 1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 2^{1024}. RSA is examined in this section in some detail, beginning with an explanation of the algorithm. Then some of the computational and crypt analytical implications of RSA are examined. RSA makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to $\log_2 (n) + 1$; in practice, the block size is I bit, where $2^i < n \leq 2^{i+1}$. Encryption and decryption are of the following form, for some plaintext block M and cipher text block *C*.

$$C= M^e \bmod n \text{……………..……………………… } (1)$$

$$M= C^d \bmod n= (M^e)\ d \bmod n= M^{ed} \bmod n \text{………. } (2)$$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of PU= {e, n} and a private key of PR= {d, n}.For this algorithm to be satisfactory for public-key encryption [7].

3. Android Operating System

Android is an open system, and is free to use by anyone. A handset manufacture can use Android if they follow the agreement stated in the Software Development Kit. There are no restrictions or requirement for the handset manufacturer to share their extensions with anyone else, as there are in other open source software, if they leave the Linux Kernel as is. The Linux Kernel is under a different and more restricted license than Android. Android is a software environment and not a hardware platform, which includes an OS, built on Linux Kernel based OS hosting the Dalvik Virtual Machine. The Dalvik Virtual Machine runs Android applications as instances of the virtual machine. Android contains a rich user interface, application framework, JAVA class libraries and multimedia support. Android also comes with built in applications contacting features such as short message service functionality (messaging), Android software environment is shown in figure (2) [8].

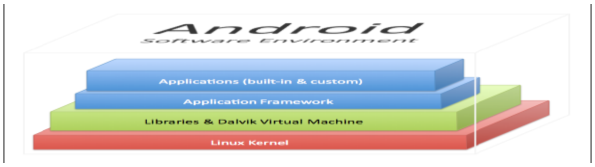

Android
Software Environment
Applications (built-in & custom)
Application Framework
Libraries & Dalvik Virtual Machine
Linux Kernel

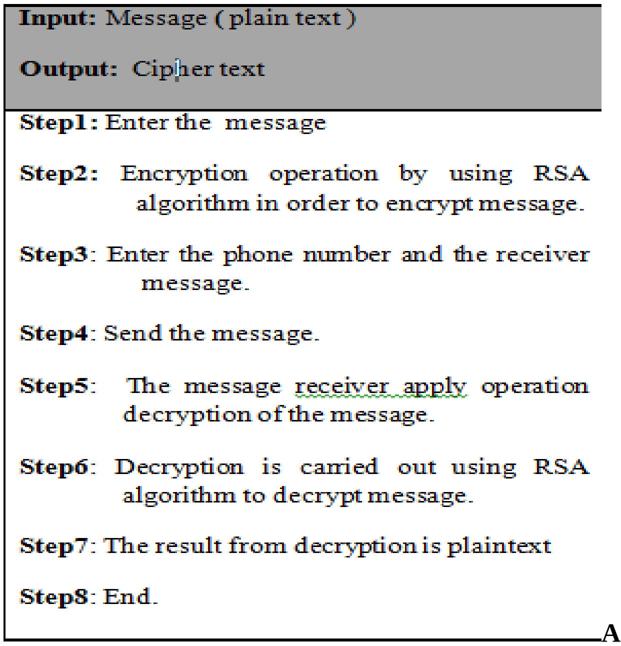
Figure 2: Android Software Environment

4. SMS messaging

SMS messaging is one of the main killer applications on a mobile phone today for some users as necessary as the phone itself. Any mobile phone you buy today should have at least SMS messaging capabilities, and nearly all users of any age know how to send and receive such messages. Android comes with a built-in SMS application that enables you to send and receive SMS messages. However, in some cases you might want to integrate SMS capabilities into your own Android application. For example, you might want to write an application that automatically sends a SMS message at regular time intervals [9].

5. The Proposed Approach

This section illustrates the proposed general algorithm for approach. It is shown in algorithm (1).



Input: Message (plain text)

Output: Cipher text

Step1: Enter the message

Step2: Encryption operation by using RSA algorithm in order to encrypt message.

Step3: Enter the phone number and the receiver message.

Step4: Send the message.

Step5: The message receiver apply operation decryption of the message.

Step6: Decryption is carried out using RSA algorithm to decrypt message.

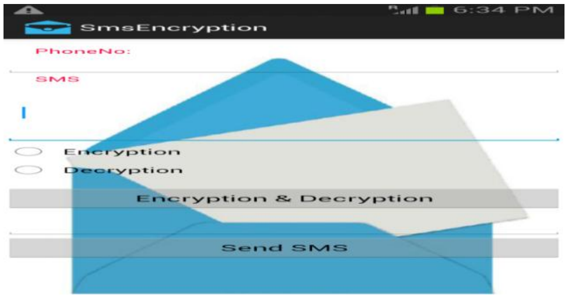
Step7: The result from decryption is plaintext

Step8: End.

Algorithm 1: General Algorithm of Proposed Approach

6. Experimental Work

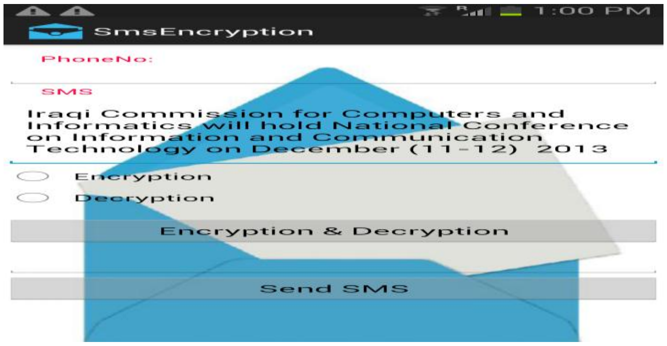
Each step in algorithm (1) will be described in the following example, the main interface of the proposed system is content five parts (phone No., SMS, choice encryption or decryption, encryption & decryption send SMS), shown in figure (3).



○ Encryption
○ Decryption

Figure 3: The Main Interface of the Proposed System

Step1: The message **"Iraqi Commission for Computers and Informatics will hold National Conference on Information and Communication Technology on December (11-12) 2013"** is entered as shown in Figure (4).

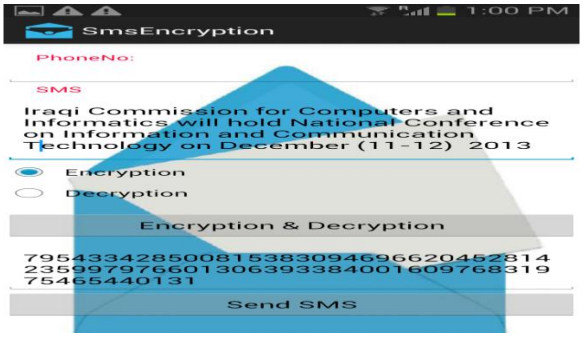


Iraqi Commission for Computers and Informatics will hold National Conference on Information and Communication Technology on December (11-12) 2013

○ Encryption
○ Decryption

Figure (4): the Message is Entered

Step2: Encryption of the message **"Iraqi Commission for Computers and Informatics will hold National Conference on Information and Communication Technology on December (11-12) 2013"** using RSA algorithm, the result **"79543342850081538309469662045281423599797660130639338400160976831975465440131"**isCipher text as Illustrated in Figure (5).



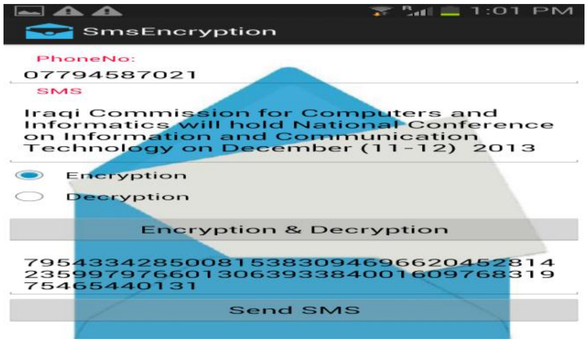
Iraqi Commission for Computers and Informatics will hold National Conference on Information and Communication Technology on December (11-12) 2013

● Encryption
○ Decryption

7954334285008153830946966204528142359979766013063933840016097683197546544013 1

Figure 5: Encryption of the Message

Step 3: enter the phone number of the receive message, as illustrated in Figure (6).



07794587021

Iraqi Commission for Computers and Informatics will hold National Conference on Information and Communication Technology on December (11-12) 2013

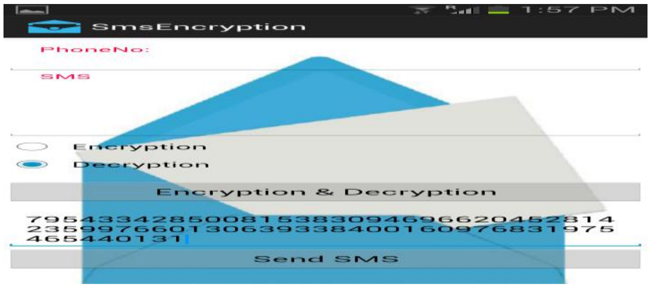
● Encryption
○ Decryption

79543342850081538309469662045281423599797660130639338400160976831975465440131

Figure 6: Enter the Phone Number

Step4: Click on the send SMS, to send the message of the receiver, as illustrated in Figure (6).

Step 5: after access the message for receiver will make decryption the message by copying the message in the part encryption & decryption and choice decryption as illustrated in Figure (7).

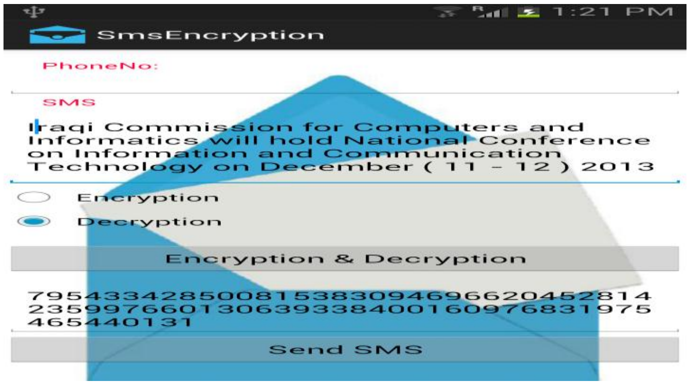


○ Encryption
● Decryption

795433428500815383094696620452814235997660130639338400160976831975 4654440131

Figure 7: Enter the Cipher text and Choice the Decryption

Step 6: The result from decryption is plaintext, as illustrated in Figure (8).



Iraqi Commission for Computers and Informatics will hold National Conference on Information and Communication Technology on December (11 - 12) 2013

795433428500815383094696620452814
235997660130639338400160976831975
465440131

Figure 8: Plaintext is the Result

Step 7: End.

7. Conclusions

1. This paper presents a method for encryption SMS messages of mobile in the Android operating system environment.
2. This method is especially designed for SMS messages.
3. The approach is compatible with any type of mobile phone that use Android operating system.
4. The execution of the approach in the mobile phone is faster and added another layer of security by using RSA algorithm.

References

[1] Hall S. P. and Anderson E., **"operating systems for mobile computing"**, Journal of Computing Sciences in Colleges. December 2009.

[2] Papapanagiotou K., Kellinis E., Marias G.F., and Georgiadis P., **"Alternatives for Multimedia Messaging System Steganography"**, Proceedings the IEEE International Conference on Computational Intelligence and Security (CIS 2005).

[3] Kumar M. and Lal S., "**A Cryptographic study of some digital signature scheme**", Ph.D.Thesis, Fomerly Agera University, 2003.

[4] Piper F. and Murphy S., "**Cryptography: A very short introduction**", Oxford university press, 2002. http:// www.Books24×7.com/Refrenceware for professionals.htm.

[5]Wikipedia,**"Encryption"** http://en.wikipedia.org/wiki/Encryption, modified on 13 December 2006.

[6] Freeman J., Neely R., and Megalo L.**"Developing Secure Systems: Issues and Solutions"**. IEEE Journal of Computer and Communication. 1998.

[7] William S, **"Cryptography and Network Security Principles and Practice"** fifth edition. 2011.

[8] Android. **"What is Android?"** http:// developer.android.com/guide/basics/what-is android.html,retrieved March 4, 2010.

[9] Wei- Meng Lee, **"Beginning Android Application Development"**, 2011.