ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

SMS Encryption using NTRU Algorithm

[I]Er.Amanpreet Kaur, [II]Er. Navpreet Singh
[I]Dept. of Computer Science Engineering GIMET, Amritsar, Punjab, India
[II]Dept. of Electronics and Communication Engineering GIMET, Amritsar, Punjab, India

Abstract
NTRU a fast encryption algorithm was yet not implemented on chat applications. The main advantage of this algorithm is fast encryption and decryption. Since chat application needs to maintain the reliability of speed within them so its also necessary to keep in mind the security measures as well as reliability matters. The NTRU fits in all results. The execution time of proposed system is less. The decryption time is reduced.

Keywords
Message Encryption, Android, Security, NTRU, Cryptography

I. Introduction

NTRU technology was written by Don Coppersmith and Adi Shamir, two of the world's leading cryptographers. In that paper ("Lattice attacks on NTRU", really an *analysis* of lattice attacks on NTRU), they noted that the best way to attack the NTRU cryptosystem was via the techniques of lattice reduction and proposed and studied one such attack. This is completely analogous to noting that the best way to attack RSA is via factoring the modulus (or that the best way to attack ECC is via the Pollard rho method), and that different-size keys give different levels of security

A. Message Encryption

Short Message Service (SMS) or Message Encryption is getting more popular now-a-days. SMS was first used in December 1992, when Neil Papworth, a 22-year-old test engineer used a personal computer to send the text message "Merry Christmas" via the Vodafone GSM network to the phone of Richard Jarvis in the UK. Presently many business organizations use SMS for their business purposes. SMS's security has become a major concern for business organizations and customers [1].
There is a need for an end to end SMS Encryption in order to provide a secure medium for communication. Security is main concern for any business company such as banks who will provide these mobile banking services. Till now there is no such scheme that provides complete SMSs security. The transmission of an SMS in GSM network is not secure at all. Therefore it is desirable to secure SMS for business purposes by additional encryption [2].
SMS Message Service (SMS) is a textual form of communication which is of precise length. SMS's are very much in use. So it is must to secure SMS's . There are various methods to secure SMS. One of them is cryptography. Cryptography has always been an important task. The main goal of every cryptographic activity is Data Security. Cryptography encodes messages in such a way, that only the sender and the receiver can understand it. Cryptographic algorithm is used to do encryption and decryption [3]. Cryptographic algorithms, also called Ciphers are classified as either symmetric or asymmetric :

1. Symmetric key encryption

Symmetric encryption is also known as private-key cryptography, and is called so because the key used to encrypt and decrypt the message must remain secure, because anyone with access to it can decrypt the data. Using this method, a sender encrypts the data with one key, sends the data (the ciphertext) and then the receiver uses the key to decrypt the data.

2. Asymmetric key encryption

Asymmetric encryption, or public-key cryptography, is different than the previous method because it uses two keys for encryption or decryption (it has the potential to be more secure as such). With this method, a public key is freely available to everyone and is used to encrypt messages, and a different, private key is used by the recipient to decrypt messages [2, 3].
There are a lot of asymmetric encryption techniques but the commonly used in the literature are Rivest, Shamir and Adleman (RSA), EL Gamal3DES Advance Encryption standard (AES), Blowfish and NTRU This study introduces SMS, its security threats and the use of asymmetric encryption technique in securing SMS [4].
The NTRU public key cryptosystem was developed in 1996 at Brown University by three mathematicians J. Hoffstein, J.Pipher and J.H. Silverman[1]. The major advantages of NTRU cryptosystem is much faster generating key, encryption time and decryption time as compared to others. It is easily compatible with mobile devices and other portable devices. It will improve the current security level and fastest speed with respect to key generation, encryption decryption with small key size. This proposal will suitable to any kind of mobile device for SMS communication with suitable data security.

B. Programming platform for mobile phones

1. Android

Android is one of today's most popular terms in the world of mobile operation systems. Android phones and Android applications are so popular among people that they have established a secured position among users in the world of mobile phones. Android is the software stack for a mobile device that includes an operating system, middleware and key applications .It is a Linux based operating system. Android Inc was founded in 2003 in Palo Alto, California, the United States in October, 2003 by Andy Rubin, Rich Miner and some other workers [5].
Android is a free and rapidly growing mobile platform. It also provides a rich platform for third-party developers to build innovative applications with its available set of APIs. (Application Programming Interfaces) Android offers a complete platform to mobile operators, developers, and handset manufacturers for constructing world-class innovative devices, software, and services [5].

2. Android Architecture

The Android operating system can be divided into five major

layers: Application, Application Framework, Libraries, Android Runtime and Linux kernel. These are the basic components that an Android application consists of. Applications are the top layer of the architecture. This is the layer where the core applications of a device such as phone calls, an email client, SMS program, calendar, maps, browser, contacts, and others can be found. These applications are written in Java and other languages [6]. The Application Framework is the second layer of the architecture. This is the framework or the outline that a developer has to follow during application development. Developers are given full access to the same framework Application Programming Interface (API) as used by the Applications layer. This layer is just like a basic tool that can be used by a developer to develop much more complex applications [6, 7].

The third layer of the architecture is libraries. It consists of sets of C/C++ libraries used by various components of the Android system. A variety of libraries are included, from the Surface Manager to libc, written in multiple languages these libraries are available to a developer for use through Application Framework. Some of these libraries are Surface Manager, Media Framework and Web Kit. The fourth layer in the architecture is the Android Runtime. It consists of sets of core libraries that are available in the Java language and Dalvik Virtual Machine. DVM has been specially designed to replace it for the Android platform [8].

The last layer of the architecture is Linux Kernel. Android depends on Linux version 2.6 for the core system services such as memory management, security settings, power management software and several drivers for hardware, file system access, networking and inter-process- communication. The Kernel also acts as abstraction layer between hardware and the rest of the software stack [9].

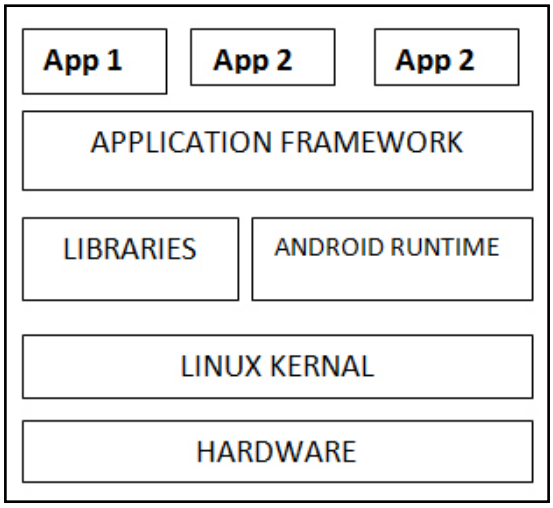

Fig.1 : Block diagram of android operating system‘s architecture.

C. Android Application Components

1. Applications

Android architecture is flexible enough to allow an application to make use of features that have already built by other applications. The Figure 1.shows four basic apps (App 1, App 2, App 3 and App 4), just to give the idea that there can be multiple applications sitting on top of Android. These apps are developed in Java, and are installed directly, without the need to integrate with Android OS [6].

2. Application Framework

Any application can make use of the capabilities of a component and also publish its own capabilities. Every application has underlying components, including:

Views: Consisting of buttons, lists, text boxes and a web browser all used to build an application.

An Activity Manager: That controls navigation and manages the life cycle of an application.

Notification Manager: That enables all applications to have notifications displayed as alerts in the status bar.

A Resource Manager: Providing access to non-code resources such as localized strings, graphics, and layout files.

Content Providers: That enables applications to share their own, and access data from other applications [10].

3. Android Runtime

In this section, all the android applications are executed. The Android runtime consists of the Dalvik Virtual Machine. It is basically a virtual machine which is used to execute the android application.. Besides the Dalvik Virtual Machine, it also consists of the core libraries, which are Java libraries and are available for all devices [10].

4. Kernel

The Android OS is derived from Linux Kernel 2.6 and is actually created from Linux source, compiled for mobile devices. A kernel acts as a bridge between hardware and software. It setups cache protected memory, scheduling and loads drivers. It provides service like power management, memory management, security etc. It helps in software or hardware binding for better communication [6, 10].

II. Literature Survey

Thakur, Neha S. [13] have studied Forensic Analysis of WhatsApp on Android Smart phones. Android forensics has evolved over time offering significant opportunities and exciting challenges. On one hand, being an open source platform Android is giving developers the freedom to contribute to the rapid growth of the Android market whereas on the other hand Android users may not be aware of the security and privacy implications of installing these applications on their phones. Users may assume that a password-locked device protects their personal information, but applications may retain private information on devices, in ways that users might not anticipate.

William Enck et.al. [14] have proposed Android Application Security. The fluidity of application markets complicate smart phone security. Although recent efforts have shed light on particular security issues, there remains little insight into broader security 1 of the application. Moving forward, we foresee ded and our analysis specifications as enabling technologies that will open new doors for application certification. However, the integration of these technologies into an application certification process requires overcoming logistical and technical challenges.

Yashpal Mote et.al.[16] have analyzed Superior Security Data Encryption Algorithm (NTRU). This Paper’s main contribution is confidentiality, integrity and authentication in SMS (Short Message Services). The transmission of an SMS in GSM network is not secure, therefore it is desirable to Secure SMS by additional encryption. In the following text, there are various algorithms are compared in the use of cryptography for SMS transfer securing.

Rohan Rayarikar et.al.[17] have studied the SMS Encryption using

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

AES Algorithm on Android. Encryption is of prime importance when confidential data is transmitted over the network. Varied encryption algorithms like AES, DES, RC4 and others are available for the same. The most widely accepted algorithm is AES algorithm. We have developed an application on Android platform which allows the user to encrypt the messages before it is transmitted over the network. We have used the Advanced Encryption Standards algorithm for encryption and decryption of the data.

III. Problem Formulation

Mobile phones are part of our daily life. Nowadays, Mobile phones provide us not only communication Services, but also many multimedia and other Function useful for human being. Mobile phones contain private or personal Data. This data is saved in a form of phone contacts, SMS, notices in a calendar, photos etc. Protection of the information depends also on a concrete user. The User should prevent against property of her/his with mobile phone. If the mobile phone is in wrong hands, most of the important information is available without a great effort (Received SMS). User registers the theft of the mobile phone almost immediately, but tapping not happens. The SMS tapping is possible in GSM network at some places. There could be used the encryption for securing of SMS. Encryption is most often realized through some user encryption applications. Therefore, there is a need to provide an additional encryption on the transmitted messages. Encryption can be classified into two categories Symmetric and Asymmetric. Symmetric encryption is the process where a single key is used for both encryption and decryption. It is somehow insecure to use. Asymmetric encryption uses two related keys, one for encryption and the other for decryption. One of the keys can be announced to the public as the public key and another kept secret as the private key. The major disadvantage of symmetric encryption is the key distribution that is mostly done through a third party. Key distribution through third party can negate the essence of encryption if the key compromised by the third party. Hence, Papers study is based on the use of asymmetric encryption technique in securing SMS. There are a lot of asymmetric encryption techniques but the commonly used in the literature are Rivest, Shamir and Adleman (RSA), EL Gamal3DES Advance Encryption standard (AES), Blowfish and NTRU. Due to this reason, in this study of the mentioned algorithms have been done. This study introduces SMS, its security threats and the use of asymmetric encryption technique in securing SMS [16].

A. Data encryption Algorithms:

DES: (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It is based on the IBM proposed algorithm called Lucifer. DES became a standard in 1974. Since that time, many attacks and methods recorded that exploit weaknesses of DES, which made it an insecure block cipher. DES: As an enhancement of DES, the3DES (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods [16].

B. Advanced Encryption Standard:

AES is the new encryption standard recommended by NIST to replace DES. It was originally called Rijndael (pronounced Rain Doll). It was selected in 1997 after a competition to select the best encryption standard. It has variable key length of 128, 192, or 256 bits; default 256. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices Brute force attack is The only effective attack known against it, in which the attacker tries to test all the

Table 1. Comparison of NTRU and RSA cryptosystems [1]

Features	NTRU	RSA
Key size	Very small	Small
Key Generation	200 times faster than RSA	Slow
Encryption/sec	1113 times faster than 204=8 RSA	Slow
Decryption/sec	1132 ms for NTRU-251	35102 ms for RSA-1024
Computation power	Too less than compared to both mobile and smart cards	Much more compared to NTRU
Speed	Faster	Slow
Efficiency	Fastest	Slow

The NTRU encryption scheme is an interesting alternative to well-established Encryption schemes such as, RSA, DES, ElGamal, and ECIES [5]. The security of NTRU depends on the hardness of computing short lattice vectors and thus is a promising user for being quantum computer resistant. There has been extensive research on efficient implementation of the NTRU encryption scheme. In this paper, we present a new algorithm for showing the performance of NTRU. The proposed method is faster on average than the performance of NTRU. The proposed method is faster on average than the best previously known procedures [16].

Table 2. RSA, ECC and NTRU performance on servers (800 MHz Pentium III) and PDAs

	Server		PDA	
	Encryption (blocks per sec)	Decryption (blocks per sec)	Encryption (blocks per sec)	Decryption (blocks per sec)
1024-bit RSA	1280	110	0.5	0.036
163-bit ECC	458	702	0.4	1.3
N=251 NTRU	22727	10869	21	12

NTRU stands for Number Theory Research Unit. NTRU is actually a parameterized family of cryptosystems; each system is specified by three integer parameters (N, p, q) which represent the maximal degree N-1 for all polynomials in the truncated ring R, a small modulus and a large modulus, respectively, where it is assumed that N is prime, q is always larger than p, and p and q are co prime. The NTRU algorithm involves three steps: key

generation, encryption and decryption, throughput [25].

IV. Results and Discussions

In this paper we have discussed about SMS security, SMS encryption, types of programming platforms for mobile phones and NTRU cryptosystems. From the above mentioned last 2 tables, we concluded that NTRU cryptosystem is faster and providing stronger security than other traditional (example RSA and ECC in both server and PDA) cryptosystems. We are expecting that it will be efficient scheme and provided better result so it will improve the current security level, fastest speed and provide reliable message at receiver end with respect to key generation, encryption decryption with small key size. Our future work is to implement NTRU crypto algorithm in our proposed model and compare with traditional cryptosystem with respect to key generation time, encryption time &decryption time for testing purpose

Step1: Registration of new user:

Step 2: user's sign in

Step 3: User enter his name

Step 4: sending message to the server by user

Step 5 message displays no of bytes used

This Section will show the result obtained from the simulated environment for NTRU, DES and RSA algorithms. Results of the simulation have been shown below in the form of graphs Throughput of the encryption algorithms is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm. Thus, if throughput increased than power consumption decreased. So, as encryption speed of the NTRU is more than the encryption speed of RSA and DES.

V.Conclusion

NTRU a fast encryption algorithm was yet not implemented on chat applications. The main advantage of this algorithm is fast encryption and decryption. Since chat application needs to maintain the reliability of speed within them so its also necessary to keep

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

in mind the security measures as well as reliability matters. The NTRU fits in all results. The execution time of proposed system is less. The decryption time is reduced. The throughput factor came out to be less which is beneficial for the battery consumption. In future this NTRU can have a good scope of research. It can be compared with RSA and AES standard encryption algorithms in Chat application on android operating system environment.

VI. AcknowledgEment

I consider myself exceptionally fortunate that I had indulged guides, learned philosopher's and caring friends to successful steer me through one of the most challenging assignment of my academic career. Today when my endeavour has reached its fruition, I look back in mute gratitude to one and all without whose help I am sure; this reality would have remained a dream

References

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

[2] *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.*

[3] *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*

[4] *Vishwa gupta,Ravindra Gupta and Gajendra Singh, "Advance cryptography algorithm for improving data security" International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 1, pp 567-578,2012.*

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

[6] *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*

[7] *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.*

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

[9] *Vaibhav Kumar Sarkania, " Android Internals" International Journal of Advanced Research in Computer Science and Software Engineering, ISSN 2277 128X, Volume 3, Issue 6, pp 143-147,2013*

[10] *Kirandeep, "Implementing Security on Android Application" The International Journal of Engineering and Science (IJES), ISSN: 2319 – 1813, ISBN: 2319 – 1805,Volume 2, Issue 3,pp 56-59 ,2013.*

[11] *Md.Alamgir Kabir, "Life Cycle Implementation of an Android Application for Self-Communication with Increasing Efficiency, Storage Space and High Performance" Green University Review, ISSN 2218-5283, Volume 3, Number 2, pp 74-78,2012.*

[12] *Giovanni Caire :Jade Programming For Android, 2012.*

[13] *Thakur, Neha S, "Forensic Analysis of WhatsApp on Android Smartphones" International Journal of Computer Applications , ISSN 0975-8887,volume 68,no.8,pp 38-44,2013.*

[14] *William Enck : A Study of Android application Security, USENIX Security Symposium August 2011.*

[15] *Rohan Rayarikar, Sanket Upadhyay and Priyanka Pimpale, " SMS Encryption using AES Algorithm on Android" International Journal of Computer Applications, ISBN 0975 – 8887, Volume 50, No.19, pp 12-17,July 2012.*

[16] *Yashpal Mote, Paritosh Nehete, Shekhar Gaikwad Guides, Ms. Sujata Tapkir and Mrs. Manjusha Yeola, " Superior Security Data Encryption Algorithm (NTRU)", An International Journal of Engineering Sciences ISSN: 2229-6913,volume 6,pp 171-181, 2007.*

[17] *Rohan Rayarikar and Sanket Upadhyay, "SMS Encryption using AES Algorithm on Android" International Journal of Computer Applications, ISBN 0975 – 8887, Volume 50, No.19,PP 12-17 July 2012.*

[18] *Jianye Liu ," Research on Development of Android Applications Intelligent Networks and Intelligent Systems (ICINIS), ISBN: 978-1-4577-1626-3,Volume 2, pp 69-72,2011.*

[19] *Avinash Bamane, "Enhanced Chat Application" Global Journal of Computer Science and Technology Network, Web & Security, ISSN: 0975-4172,Volume 12, Issue 11 ,pp 7-12,June 2012.*

[20] *Aditya Mahajan, "Forensic Analysis of Instant Messenger Applications on Android Devices" International Journal of Computer Applications ,ISBN 0975 – 8887 ,Volume 68 No.8,pp 39-44, April 2013.*

[21] *David Vronay, "Streaming Media Interfaces for Chat" Virtual Worlds Group, Microsoft Research One Microsoft Way, Redmond, WA, 98052.*

[22] *Manisha Madhwanib,Kavyashree C.V and Dr.Jossy P.George, " Cryptography On Android Message Application Using Look Up Table And Dynamic Key (Cama)" IOSR Journal of Computer Engineering (IOSRJCE) ,ISSN: 2278-0661, ISBN: 2278-8727, Volume 6, Issue 2 , PP 54-59,2012*

[23] *Mr.Nisarga Chand, Mr.Bappadittya Roy and Mr.KrishanuKundu, "Designing of an Encryption Technique Suitable For Wireless Ad-Hoc Sensor Network" International Journal of Advanced Research in Computer Science and Software Engineering, , ISSN: 2277 128X, Volume 3, Issue 3,pp 632-637, March 2013.*

[24] *Yashpal Mote, Paritosh Nehete, Shekhar Gaikwad Guides, Ms. Sujata Tapkir and Mrs. Manjusha Yeola, " Superior Security Data Encryption Algorithm (NTRU)", ISSN: 2229-6913,Volume 6, pp 171-181,2012.*

[25] *Mr.Sachin Majithia, " Implementation of NTRU on Cloud Network in an Android Platform and Comparison with DES and RSA" International Journal of Advanced Research in Computer Science and Software Engineering, volume 3,Issue 11, pp. 100-105,2013.*