International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-1, January 2016
ISSN: 2395-3470
www.ijseas.com

SMS Encryption using NTRU Algorithms on Android Application

***Shobha Jha[1], *U. Dutta [2], **Priyank gupta [3]**

**Computer Science and Engineering Department, Maharana Pratap College of technology*
Putli Ghar Road, Near Collectorate, Gwalior-474006, Madhya Pradesh, India

***SOS in Mathematics and Allied Sciences, Jiwaji University,Gwalior-474001, Madhya Pradesh, India*

[1]shobhajh@gmail.com, [2]unmukh62@hotmail.com, [3]guptapriyank87@gmail.com

ABSTRACT- In these days, security is necessary for all the applications on the network. Number of techniques and algorithms are used for the purpose of providing the security in many fields by many approaches. NTRU is a fast encryption algorithm and it is implemented in various fields but it was yet not implemented on SMS applications on android application. For providing the security to the data transferred on the network, NTRU algorithm is seen as fast and best algorithm. NTRU is patented and an open source public-key cryptosystem in which lattice-based cryptography system is used for encryption and decryption of files. Many applications make use of extensive databases (chats) to store the data and are accessible from anywhere by the multiple people simultaneously via mobile networks or towers. This paper represents the implementation of the NTRU algorithm for security of such application that is used for chats and showed that this algorithm provides the best security for android chatting application as well as systems chatting application. The keys generated by the server are used for encryption/decryption of files and encrypted files are stored in the database. This paper focuses on implementation an algorithm for chat application on android.

Keywords- Message Encryption, Android, Security, NTRU, Cryptography

I. INTRODUCTION

Online chat may refer to any kind of communication over the internet that offers a real-time transmission of text messages, images as well as audio-video files from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly to save time and other resources. Thereby, a feeling similar to a spoken conversation is created. Which distinguishes chatting from other text-based online communication forms such as internet forums and email. Online chat may address point-to-point communications as well as multicast communications from one sender to many receivers and voice-video chat, or may be a feature of a web conferencing service.

Online chat in a less stringent definition may be primarily any direct text-based or video-based (webcams), one-to-one chat or one-to-many group chat using tools such as instant messengers. The expression online chat comes from the word chat which means “informal conversation”. Online chat includes web-based applications that allow communication-often directly addressed, but anonymous between users in a multi-user environment. Web conferencing is a more specific online service, that is often sold as a service, hosted on a web server controlled by the vendor.

File NTRU technology was written by Don Coppersmith and Adi Shamir, two of the world’s leading cryptographers. The proposed 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 nothing 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). In this paper we proposed a chat application with cryptography technique using NTRU algorithm that is called NTRU to secure message transmission from sender to receiver.

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 cipher text) 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].

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 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

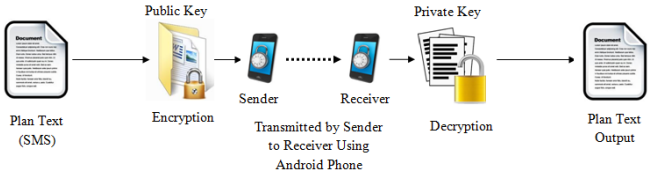
network. We have used the Advanced Encryption Standards algorithm for encryption and decryption of the data.

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].

IV. Overview of NTRU Algorithm

NTRU(N-th degree Truncated polynomial Ring Unit) is an open source and patented public-key cryptosystem which uses lattice-based cryptography for encryption and decryption of text. The two keys used in this algorithm are (i) public key and (ii) private key. The key is used for the encryption is public key or to verify the digital signature but private key is used for decryption or to create digital signature, as shown in Fig. 1 [26]



It is based on polynomial arithmetic; therefore it provides very fast computation for the encryption and decryption of the message. NTRU has less complexity i.e. $O(N^2)$ [27,28]. The operations are based on objects that are in a polynomial ring:

$$R = Z[X] / (X^N - 1)$$

The polynomials, present in the ring have integer coefficients and degree N-1:

$$a = a_0 + a_1X + a_2X^2 + \ldots + a_{N-2}X^{N-2} + a_{N-1}X^{N-1}$$

Actually the NTRU is a parameterized family of cryptosystems; in which each systems is defined by three parameters (N, p, q), which represents the maximum degree N-1 for all of the polynomials in the ring R, small where p and q are co-prime. Suppose f, g, r, e, and a are all ring polynomials.

A. **Key Generation:** NTRU involves a public key and a private key. The public key is used for encryption message and can be known to everyone. Messages encrypted with this key can only be decrypted in a reasonable amount of time using the private key.

B. **Encryption:** For encryption of a plaintext message m ε R using h as the public key, Alice chooses a random element r ε R and creates the ciphertext:

$$E = r * h + m \pmod q$$

C. Decryption: For decryption of the ciphertext e using the f as a private key, Bob firstly computers the value:

$$a = f * e \pmod q$$

Bob then selects a ε R to satisfy this congruence and to lie in a certain pre-specified subset of R. He next does the mode p computation $f_q^{-1} * a \pmod p$ and the value he calculates is equal to m modulo p[29].

The main characteristics of NTRU algorithm are low computational and memory requirements for providing a high level security. In this algorithm the difficulty is faced during the factorization of the polynomials into two different polynomials having very less coefficients. NTRU is a widely

usable, well-accomplished and promising cryptosystem.

V. Proposed Work

In Current or Existing work, NTRU algorithm was implemented on an android platform as well as on N-tier architecture where multiple servers' exits like job portal application where job seekers, recruiters and admin are present. But NTRU algorithm has not been implemented on encrypted SMS on android mobiles. Challenge is to secure SMS transfer from sender to receiver as well as save time.

The first objective of proposed work is to study the various encryption/decryption algorithms either they are asymmetric or symmetric. Symmetric key algorithms are those in which use the same key for the encryption and decryption of data but in this asymmetric key algorithms, the key which is used for encryption of data is not same with the key used for decryption of data. The next objective is to design the encrypted SMS on android mobile phone from sender to receiver, and also used to decrypt encrypted SMS sent from sender's side using private key. The last objective is to analyze or check encrypted and decrypted SMS are same or not. And also analyze the results of proposed work.

VI. Proposed Algorithm

The research methodology in this paper is divided into 6 steps as shown in Fig.2 which arhieve our desired goal from sender's side:

Step1: In this phase, we have to open message box to type the message.

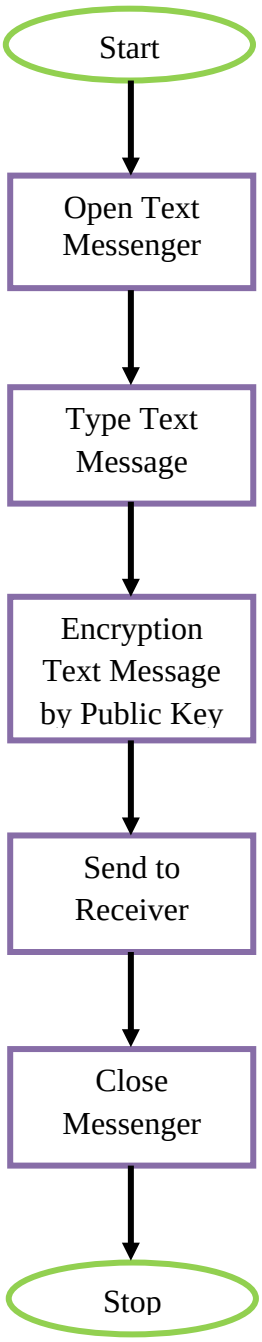
Step2: In this step sender type the plan text message or SMS which is send to receiver.

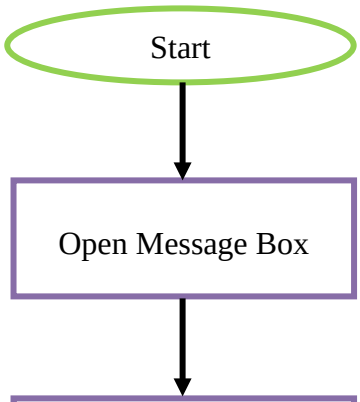
Step3: This phase include the encryption algorithm and convert plan text to encrypted text using public key of NTRU algorithm.

Step4: Send encrypted text to receiver if send success fully than receiver receives encrypted SMS.

Step5: In this phase receiver decrypt encrypted SMS with is sends by sender. And convert it into plan text using private key.

Step6: finally get plan text using NTRU encryption-decryption algorithm with save time.





VII. Conclusion

NTRU a fast encryption algorithm was yet not implemented on chat applications. Now I have implemented this algorithm for android application for send SMS from sender to receiver. The main advantage of this algorithm is fast encryption and decryption. Since chat application needs to maintain the reliability of speed within them so it's also necessary to keep in mind the security measures as well as reliability matters. The NTRU fits for these types of applications. The execution time of proposed system is less as compare to other encryption algorithms. As well as 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 philosophers 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.

[26] Amandeep Kaur Gill and Charanjit Sign, "Survey on Encryption Algorithms to Overcome Security Issues in Cloud Computing" International Journal of Advanced and Innovative Research(2278-7844), Volume 3, Issue 4, pp. 475-480, 2015.

[27] Ranjeet Ranjan, Dr. A. S. Baghel and Sushil Kumar, "Improvementof NTRU Crytosystem" International Journal of Advanced Research in Computer Secience and Software Engineering, Volume 2, Issue 9, pp. 79-84, 2012.

[28] http:// en.wikipedia.org/wiki/NTRU.

[29] Fei Hu Kyle Wilhelm, Michael Schab, Marcin Lukowiak, Stanislaw Radziszowski and yang Xiao, "NTRU-based sensor network security: a low-power hardware implementation perspective" Security and Communication Netwoks Copyright #1008 John Wiley & Sons, Ltd.