Commercial Application Of Cryptosystems In Mobile Services

Swati Chaudhary, Vinit Kumar, Preeti Chaudhary

Computer Science and Engineering Department,
Bhagwant University, Ajmer, Rajasthan

chaudhary.swati125@gmail.com

ABSTRACT –In this research paper we are mainly focusing on NTRU Cryptosystems in mobile services mainly Short Message Service (SMS) and its security which is getting more popular now-a-days for commercial purposes. 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. It will play a very important role in the future business areas of mobile commerce (M-Commerce). Presently many business organizations use SMS for their business purposes. SMS's security has become a major concern for business organizations and customers. 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. In this paper, we have analyzed different cryptosystems for implementing to the existing Secure Extensible and Efficient SMS (SEESMS). We planned to implement NTRU cryptosystem into existing SEESMS frame. The NTRU public key cryptosystem was developed in 1996 at Brown University by three mathematicians J. Hoffstein, J.Pipher and J.H. Silverman. It is not that much popular cryptosystems like RSA, ECC and other traditional. 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. We have compared theoretically and analysis of NTRU with RSA and ECC cryptosystems at end of my papers. It is theoretically proposed here. We are expecting our novel scheme may show better result than others. So it will provide 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.

Keywords – ECC, M-Commerce, NTRU, Performance analysis, RSA, SMS Encryption, SMS Security

I. Introduction

SMS stands for Short Message Service. In 1992, the first SMS technology enables the sending and receiving of messages between mobile phones. SMS message contains at most 140 bytes (1120 bits) of data, so any one SMS message can contain up to 160 characters (if 7-bit character encoding is used) and 70 characters (if 16-bit Unicode UCS2 character encoding is used). SMS provides a convenient means for people to communicate with each other using text messages via mobile devices or Internet connected computers. It is possible to send ringtones, pictures, operator logos, wallpapers, animations, business cards and WAP configurations to a mobile phone with SMS messages. One major advantage of SMS is that it is supported by 100% GSM mobile phones. Almost all subscription plans provided by wireless carriers include inexpensive SMS messaging service. The mobile messaging market is growing rapidly and is a very profitable business for mobile operators. It can be seen from Table I that the growth rate of SMS in worldwide during 2000 – 2015F (F stands for forecast) in billion. This table implies that the use of SMS rapidly increasing. It may further increase because many organizations are using as communication media between customer and banking organizations, schools and others.

SMS is getting more popular now-a-days. It will play a very important role in the future business areas of mobile commerce (M-Commerce). Up to now many business organizations use SMS for their business purposes

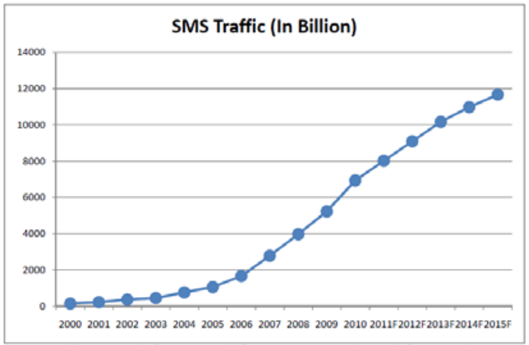

Table 1: Growth of SMS – World from 2000 to 2015F (F stands for Forecast)
Source: Portio Research Ltd.

SMS's security has become a major concern for business organizations and customers. 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. Currently there is no such scheme that provides complete SMSs security.

SMS has a variety of advantages and disadvantages for M-Commerce purpose. The advantages are easy to use, common messaging tool among consumers, works across all wireless operators, affordable for mobile users, no specific software required to installation, allows banks and financial institutions to provide real-time information to consumers & employees, stored messages can be accessed without a network connection. Very few disadvantages are text data and limited up to 140-160 characters per message, does not offer a secure environment for confidential data during transmission and there is no standard procedure to certify the SMS sender. Presently researchers proposed some security concepts regarding SMS security. Most of the proposals are software frames to be installed on mobile device and /or on the SIM cards to implement security.

This paper proposed some idea regarding to exchange SMS in secure manner at peers' level. It requires a software framework to certify the phone numbers of both sender & receiver. Here users are allowed to choose cryptosystems and security parameters for transmitting secure message to achieve better cost and efficiency of the operation.

Rest of paper is organized as follows. Section II provides an overview of related work. Section III discussed about SMS security. Section IV presents briefly about SMS encryption. Section V discusses analyzed types of programming platforms for mobile phones. Section VI brief discuss about NTRU cryptosystems. Section VII represents the result of application of novel scheme and followed by discussion and future work.

II.Related Work

Particularly about secure extensible and efficient SMS (SEESMS), the proposal presented by Alfredo De Santis and his team members in [1] which designed a Java based framework for exchanging secure SMS. They considered RSA, DSA and ECDSA algorithms. Here we have considered the same SEESMS frame with NTRU cryptosystems for SMS security purpose.

III. SMS SECURITY

Now-a-days, SMS is used for M-Commerce purpose. SMS will play a very vital role in the future banking or commercial purpose because of its simplicity and cheapness. Upcoming payment system will be based on the mobile device by using SMS. Money can be debited or credited from the bank through the SMS by using the GSM network. But some security related services of SMS should be available when we go for such m-commerce or m-banking.

Network operators are demanding spam control and anti-spoofing capabilities to protect their SMS network and subscribers. When customers have complaints regarding SMS, operators do have not any other options to block such types of SMS rather than blocking such SMS subscribers.

There are some security gaps for SMS. Such as Snooping, SMS Interception, Spoofing, Modification, Faking, Flooding, Spam and other SMS-related scams are a global problem. There are many security threats to mobile subscribers and operators. It is easy to sneak a virus as a Trojan attachment in an SMS message.

There are many incidents of rogue operators gaining unauthorized access to the SS7 networks of major service providers and routing millions of text messages into those networks. Therefore it does congestion and blocking other genuine SMSs. So it may delay or may not reach to recipients. Quite often they are attempts at delivering massive volumes of spam into the network. Service providers often end up building new facilities to deal with the increase in messaging traffic - with no corresponding increase in revenue. Spoofing is great opportunity for fraud -coaxing users into providing sensitive personal data, which results in a financial windfall for the bad guy. In fact, there have been reports of spoofing cases where messages are sent disguised as official government announcements for emergencies.

Current trends in mobile devices are raising the probability of attack. Devices have much more functionality than they used to – they have become small computers. Currently users expect high level of security while doing mobile transactions. Some familiar problems are mentioned here for popular M-Commerce: data confidentiality while transmitting, data and application access must be controlled, data integrity, loss of device must have limited impact, and non repudiations. When SMS used for M-Commerce the following services are required :

1. Confidentiality: only the valid communicating users can view the SMS.

2. Integrity: the SMS can't be tampered by the intruders.

.

3. Non-repudiation: no party can deny the receiving or transmitting the data communicating between them.

4. Authentication: each party has to have the ability to authenticate the other party.

5. Authorization: it has to be ensured that, a party performing the transaction is entitled to perform that transaction or not.

We realized that security is most essential for mobile users and network operators to avoid different threats at different levels. 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.

IV. SMS ENCRYPTION

SMS encryption is the process of transforming SMS information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.
The result of the process is encrypted information. Encryption is also used to protect data in transit, for example data being transferred via networks mobile telephones Encrypting data in transit also helps to secure it as it is often difficult to physically secure all access to networks. Encryption can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message. Successfully using encryption to ensure security may be a challenging problem . There are so many algorithms are available for SMS encryption. The application of SMS encryption algorithms is dependent upon operating system of the types of mobile device. The other factors like energy consumption, speed, security and others are to be considered while choosing the encryption techniques.

V. Types Of Programming Platforms For Mobile Phones

All present different mobile phones using different types programming platform software for their running the user's program. Currently available software mentioned below.

ANDROID

Android is a mobile operating system initially developed by Android Inc. Android was purchased by Google in 2005.It is free and open source coding. Developers write in the Java language, controlling the device via Google-developed Java libraries. The Android operating system software stack consists of Java applications running on a Java based object oriented application framework on top of Java core libraries running on a Dalvik virtual machine featuring JIT compilation. Libraries written in C include the surface manager, Open Core media framework, SQLite relational database management system, OpenGL ES 2.0 3D graphics API, Web Kit layout engine, SGL graphics engine, SSL, and Bionic libc.

BLACKBERRY

BlackBerry is a line of mobile e-mail and smart phone devices developed and designed by Canadian company Research In Motion (RIM). BlackBerry functions as a personal digital assistant with address book, calendar, memo pad and task list capabilities. It also functions as a portable media player with support for music and video playback and camera and video capabilities. BlackBerry is primarily known for its ability to send and receive (push) Internet email wherever mobile network service coverage is present, or through Wi-Fi connectivity. BlackBerry is mainly a messaging phone with the largest array of messaging features in a smart phone today, including auto-text, auto-correct, text prediction, support for many languages, keyboard shortcuts, text emoticons, push email, push Face book, Twitter and MySpace notifications, push EBay notifications, push instant messaging with BlackBerry Messenger, Google Talk, ICQ, Windows Live Messenger, AOL Instant Messenger and Yahoo Messenger; threaded text messaging and a customizable indicator light near the top right of all Blackberry devices. BlackBerry's push gives BlackBerry devices their renowned battery life. All data on the phone is compressed through BlackBerry Internet Service (BIS) .

JAVA ME

Java Micro Edition (Java ME) is developed by Sun Microsystems. Almost all mobile phones include this programming platform. Unfortunately, the standard API is quite poor to use advanced features (such as VoIP). Code program is running on a virtual machine. This concept is hardware independent, but its computing power may not be sufficient for some applications (such as asymmetric cryptography). Common mobile phones with Java ME use MIDP profile. This profile uses CLDC configuration, which requires hardware with processor 16bit/16MHz, Therefore this cannot ensure right run in all phones.

SYMBIAN OS

Symbian OS was originally developed by Symbian Ltd. In 2008, Nokia acquired that company. It is royalty-free, open source software. This software is for mobile devices and smart phones,
with associated libraries, user interface, frameworks and reference implementations of common tools.

WINDOWS MOBILE

Windows Mobile is a mobile operating system developed by Microsoft. It's feature-wise and aesthetically designs are somewhat similar to desktop versions of Windows. Additionally, third party
software development is available for Windows Mobile, and software applications can be purchased via the Windows Marketplace for Mobile. Microsoft is phasing out Windows Mobile to specialized markets, such as rugged devices, and

focusing on its new mobile platform, Windows Phone 7.

OTHERS

There are some programming platforms are available but they have small market share in the mobile phones. These platforms are supported only by few types of mobile phones. Those are listed here: BREW, Macromedia Flash Lite, Micro browser Based, Palm OS, Qt (framework).

VI. NTRU Cryptosystems

The NTRU public key cryptosystem was developed in 1996 at Brown University by three mathematicians J. Hoff stein, J.Pipher and J.H. Silverman. NTRU encryption algorithm is a lattice-based alternative to RSA and ECC and is based on the shortest vector problem in a lattice. NTRU can be used in mobile devices and other mobile applications because of its features of easy generation of keys, high speed and low memory use. This is based on shortest vector problem in a lattice and operations based on objects in a truncated polynomial ring .

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

All polynomials in the ring have integer coefficients and degree at most N-1:

$$a=a0+a1X+a2X2+\ldots\ldots..+aN–2XN–2+aN–1XN–1=\Sigma\ aiXi$$

it can represented as vector: $a = (a0,a1,a2,\ldots,aN\text{-}2,aN\text{-}1)$.

$$b=b0+b1X+b2X2+\ldots\ldots..+bN–2XN–2+bN–1XN–1=\Sigma\ biXi$$

it can represented as vector: $b = (b0,b1,b2,\ldots,bN\text{-}2,bN\text{-}1)$.

$$a+b = \Sigma\ aiXi + \Sigma\ biXi = \Sigma\ (ai+bi)\ Xi$$
$$a*b = \Sigma\ aiXi * \Sigma\ biXi = \Sigma\ [\Sigma\ (\ aibj)]Xk$$

Another operation we should know is modular arithmetic in which:

$a \bmod c \pm b \bmod c = (a \pm b) \bmod c$;
$a \bmod c * b \bmod c = (a * b) \bmod c$.
and a = b (mod c) means a and b have the same reminder when they are divided by c.

When we do modular arithmetic to a polynomial in the ring with the integer modulus, it just means to divided each coefficient of the polynomial by the modulus and keep the reminders as the new coefficients.NTRU has 3 integer parameters: N, p, q. N represents the degree of the polynomials at most N-1; p is smaller than q. p and q are small moduli used to reduce the coefficients of the polynomials. They do not have common divisor. We briefly describe the NTRU algorithm as follows.

Key generation

We have to choose two random polynomials f and g in the ring with the restriction that their coefficients are small, usually in {-1, 0, 1}. We import another symbol here: L(d1, d2), which means a set of polynomials with d1 coefficients are 1, d2 coefficients are -1 and the rest are 0.Usually we choose f from Lf(df, df-1) and g from Lg(dg, dg-1). Then we compute fp (the inverse of f modulo p) and fq (the inverse of f modulo q) with the property that

$$f * fp = 1 \pmod p \text{ and } f * fq = 1 \pmod q.$$

If f doesn't have these inverses, another f should be chosen. The pair of polynomials f and fp should be kept as the private key, and the public key h can be computed by

$$h = pfq*g \pmod q.$$

Both f and fp are used for private key and h is used for public key.

Example: The parameters (N, p, q) have the values N = 11, p = 3 and q = 32 and therefore the polynomials f and g are of degree at most 10. The system parameters (N, p, q) are known to everybody. The polynomials are randomly chosen, so suppose they are represented by

f= -1+X+X2-X4+X6+X9-X10
g= -1+X2+X3+X5-X8-X10

Using the Euclidean algorithm the inverse of f modulo p and modulo q, respectively, is computed So

fp= 1+2X+2X3+2X4+X5+2X7+X8+2X9 (mod 3)

fq= 5+ 9X+ 6X2+ 16X3+ 4X4+ 15X5+ 16X6+ 22X7+ 20X8+ 18X9+ 30X10 (mod 32)

Which creates the public key h computing the product

h = pfq*g (mod q).
= 8+ 25X +22X2 +20X3 +12X4 +24x5 +15X6+ 19X7 + 12X8 +19X9 +16X10 (mod 32)

Encryption

The message to be sent can be put into a form of a polynomial m ϵ Lm(dm, dm) whose degree is at most N-1. Then we randomly choose a blinding polynomial r ϵ Lr(dr, dr) in the ring. So the encrypted message e should be computed by e = r*h + m (mod q).

Example: Let m = -1+X3+X4-X8+X9+X10
r = -1 +X2+X3+X4-X5-X7

e= r*h + m (mod q)
= 14 + 11X+ 26X2+ 24X3+ 14X4+ 16X5+ 30X6+ 7X7+ 25X8+ 6X9+ 19X10 (mod 32)

Decryption

First, use a part of the private key f to compute polynomial

a = f*e (mod q), then
b = a (mod p), and then

We use the other part of the private key fp to compute polynomial

c = fp*b (mod p).

If this procedure is successful, c will be the original message m. actually, for appropriate parameter values, this probability is extremely high. The polynomial satisfies

a = f*e (mod q)
=f*(r*h + m) (mod q)
=f*(r*pfq*g + m) (mod q)
=pr*g + f*m (mod q) [f*fq=1 (mod q)].

The coefficients of r, g, f, m and the prime p are all much smaller than q, and for appropriate parameter values, the coefficients of a can be ensured lie in [-q/2, q/2], so after reduced modulo q, these coefficients are not changed. Then

b = a (mod p)
= (p*r*g + f*m) (mod p)
= f*m (mod p),
c = fp*b (mod p)
= fp*f*m (mod p)
= m (mod p) [f*fp=1 (mod p)],
so polynomial c is just the original message m.

Example
a = f*e (mod q)
= 3-7X-10X2-11X3+10X4+7X5+6X6+7X7+5X8 -9X9 – 7X10 (mod 32)

b = a (mod p)
= -X- X2+ X3+ X4+ X5+ X7- X8- X10 (mod 3)

c = fp*b (mod p)
= *-1+X3+X4-X8+X9+X10 = m* (Proved)

VII. Result

RSA and ECC cryptosystems are considered as the most popular public key cryptography algorithms. In the literature, many authors presented many weaknesses on RSA. They stated that RSA is slow [12] Hastad stated in [13] that low exponent RSA is not secure if the same message is encrypted to several receivers. In practice, RSA has proved to be quite slow. Furthermore, RSA is not well suited for limited environments like mobile phones and smart cards without RSA co-processors [14]. RSA also requires longer keys in order to be secure compared to some other cryptosystems like ECC. ECC is faster than RSA [15], ECC-160 has 6× smaller key-size than RSA-1024 and can generate a signature 12 times faster than RSA and ECC is faster, it occupies less memory space than an equivalent RSA system, ECC generates asymmetry keys pair faster than RSA, ECC is more efficient than the ubiquitous RSA based schemes because ECC utilizes smaller key sizes for equivalent security, Security wise, ECC is stronger than RSA [14]. The NTRU crypto system is a new public key cryptography approved in 2009. The table II gives the total comparison between NTRU and RSA.

The company www.securityinnovation.com has built a cryptographic toolkit called NERI that is based on the NTRU algorithm. It provides data that compare the performance of NTRU with that of RSA and ECC on both servers and PDAs . It implies that NTRU to have a performance advantage that ranges from 9:1 in the case of NTRU: ECC decryption on PDA to over 333:1 in the case of NTRU: RSA decryption on PDA.

In case of mobile device, this NTRU crypto algorithm already had performed tests on key generation, encryption and decryption, as well as signing and verifying operations for one hundred times and then calculated the average of time required for each operation in They used java emulator. They had considered four of Nokia devices such as Nokia N70, N73, N93 and Nokia 5800 Xpress Music. The table IV has shown its comparison. From the results, they noticed that NTRU algorithm performed very well on the mobile devices and there were no negative effects on the mobile devices' performance due to the small time required for the key generation. NTRU does not require high computing power, which makes it the best alternatives for mobile devices with providing either same or more security facility. Figure 1 shows the proposed public key cryptography implementation in non-server architecture based on NTRU algorithm.

NTRU cryptosystem is gaining more popularity slowly because it's key size is very small, key generation, encryption speed, decryption speed are much faster and computation power requires
very less, Operation speed is very fast, more efficient, consuming less space and more suitable for mobile devices (shown in table II). It is not free (as per my knowledge). It is standardized in IEEE 1363.1-2008 and X9.98-2010. Unlike RSA and ECC, NTRU is resistant to quantum computing based on crypto attacks. It is the smallest public key crypto available on market (8 kb). Some constraints are i) no support for NTRU in the leading browsers and ii) it is necessary required to implement NTRU at both ends of the SSL tunnel. www.securityinnovation.com provides SSL libraries and software development toolkits in C/C++ and Java. Unlike RSA and ECC, no successful attack has been recorded to break the security of this algorithm [14].

From the above, we hope that NTRU crypto algorithm will be more suitable and easy to implement in mobile device for our proposed scheme.

VIII. Discussion And Future Work

Now-a-days SMS is more popular for different applications in our daily real life. Errorless data transmission with secured is important in wireless environment. 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 3 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.

IX References

[1] *De Santis, A. Castiglione, A. Cattaneo, G. Cembalo, M. Petagna, F. Petrillo, U.F, "An Extensible Framework for Efficient Secure SMS," Complex, Intelligent and Software Intensive Systems (CISIS), International Conference, 15-18 Feb.2010, pp. 843-850,doi:10.1109/CISIS.201081*

[2] Hossain, A.; Jahan, S.; Hussain, M.M.; Amin, M.R.; Shah Newaz, S.H.; "A Proposal For Enhancing The Security System Of Short Message Service In GSM", Anti-counterfeiting, Security and Identification, 2nd International Conference, ASID 2008, doi: 10.1109/IWASID.2008.4688386

[3] http://en.wikipedia.org/wiki/Encryption

[4]ww.en.wikipedia.org/wiki/Android_%28mobile_phone_platform%

[5] http://en.wikipedia.org/wiki/BlackBerry

[6] Lisonek, David.; Drahansky, Martin.; "SMS Encryption for Mobile Communication",Security Technology, SECTECH '08, International Conference, 2008,doi:10.1109/SecTech.2008.48

[7] Agoyi, Mary; Seral, Devrim; "SMS Security: An Asymmetric Encryption Approach,"Wireless and Mobile Communications (ICWMC), 6th International Conference, 2010, pp.
448-452, doi: 10.1109/ICWMC.2010.87
[8] http://en.wikipedia.org/wiki/Mobile_application_development

[9] http://en.wikipedia.org/wiki/NTRUEncrypt

[10] J. Hoffstein, J. Pipher, J. H. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem,"Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, J.P. Buhler (ed.),Lecture Notes in Computer Science 1423, Springer-Verlag, Berlin, 1998, pp. 267-288.

[11] Xiaoyu Shen; Zhenjun Du; Rong Chen: "Research on NTRU Algorithm for Mobile Java Security", in International Conference Scalable Computing and Communications; Eighth International Conference on Embedded Computing (SCALCOM-MBEDDEDCOM'09), 2009. page(s): 366 – 369

[12] http://www.oocities.org/hmaxf_urlcr/rsa.htm

[13] Kaoru KUROSAWA, Koji OKADA and Shigeo Tsujii: "Low exponent attack against elliptic curve RSA",
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.44.2453

[14] Sameer Hasan Al-Bakri, M. L. Mat Kiah, A. A. Zaidan, B. B. Zaidan and Gazi Mahabubul Alam: "Securing peer-to-peer mobile communications using public key cryptography: New security strategy", International Journal of the Physical Sciences Vol. 6(4), pp. 930-938, 18 February, 2011

[15] http://docs.redhat.com/docs/en-US/Red_Hat_Certificate_System/8.0/html/Deployment_Guide/SSL-TLS_ecc-and-rsa.html

[16] John Welham: "Implementation and Comparison of XTR and NTRU Against Current Cryptographic Algorithms", Master of Science Thesis, Department of Computer Science,
University of Bristol, UK, September – 2002.