Implementation of E-mail Security System Using NTRU Cryptosystem and SHA-1 Algorithm

Khin Myo Kyi, Zin May Aye
University of Computer Studies (Mawlamyine)
khinmyokyi01 @gmail.com, zinmay110@gmail.com

Abstract

Security of exchanging private information over a non secure channel is important in communications system. Efficient cryptographic techniques are necessary to endow the security level in mail system. Email security is needed to implement to send the message in a secure way. With no encryption email activity is plainly visible by any occasional eavesdropper. The Number Theory Research Unit (NTRU) cryptosystem becomes the fastest and smallest public key security solutions for data communication network and application. Email has become one of the most important means of communication and it is widely used all over the world in various fields. This system intends to implement the email security system by using NTRU cryptosystem to encrypt and decrypt mail message to provide security goal of confidentiality. Secure Hash Algorithm (SHA-1) is used to check the mail message integrity of this system.

Keywords*: Confidentiality, Email security, NTRU, PKCS, SHA-1,*

1. Introduction

E-mail is one of the Internet Applications and it is the common use in the current world communication. Current world technologies continuously changes and develops. All technological developments bring some problems besides. Internet Applications are more common today. The biggest problem of these applications is security. Many processes are done by sending mails now such as corresponding in a company or corresponding internationally. The attackers can interfere with E-mails by taking these and transporting the false data to users. Mail security is necessary so it needs to protect the danger of the attackers by using cryptography method. Cryptography provides the privacy, authentication and integrity maintenance for the requirement of the transaction.

Number Theory Research Unit (NTRU) cryptosystem is a collection of mathematical algorithms based on manipulating lists of very small integers. NTRU is the first secure public key cryptosystem not based on manipulating or discrete logarithmic problems. The keys are generated by having small potent polynomials from the ring of truncated polynomials. The security of NTRU comes from the interaction of polynomial mixing modulo two relatively prime numbers. Encryption and decryption processes are extremely fast and key creation is fast and easy. SHA-1 produces a 160-bit hash value and was originally published as FIPS 180-1. The SHA-1 algorithm produces a 160-bit message digest and is therefore considered a stronger algorithm than MD5.In this system, the public key cryptosystem (NTRU) algorithm is applied to encrypt and decrypt mail message. Secure Hash Algorithm (SHA-1) is used to achieve mail message digest for data integrity.

This paper is organized as follows: In Section 2, summarizes the related work in introduction to e-mail system. In Section 3, the background theory is explained. Section 4 presents the implementation of e-mail security system. The last section; Section 5 is the conclusion.

2. Related Work

Mustafa DULGERLER[1] M. SARISAKAL[2] [2] proposed A Secure E-mail Application using the Elgamal Algorithm: MD message controller. Cryptography was used only by political or military communications for long time. NTRU is ideally suited for application where high performance, high security and low power consumption are required. NTRU has its unprecedented performance advantages open up new options for security.

JIANG Jun [1] presented a novel mutual authentication and key agreement protocol based on NTRU public key cryptography. The symmetric encryption, hash and "challenge response" techniques were adopted to build their protocol. Since the lightweight NTRU public key cryptography is employed, their protocol can not only overcome the security flaws of secret-key based authentication protocols. Cryptographers prefer using another cipher that has been proven secure such as Advanced Encryption Standard (AES) [4], Block Cipher [3] International Data Encryption algorithm (IDEA), Triple DES or SHA-256 in their cryptosystems.

PGP protocol is the e-mail security protocol which was originally developed by Philip R.Zimmerman in 1991. The services that the original

PGP gives are confidentially, authentication, e-mail compression, segmentation and reassembly [6].

In this e-mail system NTRU public key cryptosystem is applied to establish the security and providing data integrity using SHA-1 Algorithm.

2.1. Introduction to E-mail System

E-mail is widely used all over the world in various fields such as economic, office, personal case and so on. It is easy to transport data from place to place in a short time. E-mail has become one of the most important means of communication. Electronic mail, often abbreviated to e-mail, email or originally E-mail, is a store and forward method of writing, sending, receiving and saving messages over electronic communication systems.

In this e-mail system Simple Mail Transfer Protocol (SMTP) server as a local host and performed e-mail sending and receiving processes for end users. In general, when a mail is sent from a host computer in the mail system, the SMTP server will move the sent mail from one mail server to another and the email packets routed through the internet until they reach the destination mail server.

3. Public Key Cryptography (PKCS)

Public Key Cryptography Standard is more appropriate than symmetric key cryptosystems for security purposes. Public key methods are very powerful and give us much more flexibility. Public-key encryption uses a private key that must be kept secret from unauthorized users and a public key that can be made public to anyone. The public key and the private key are mathematically linked; data that is encrypted with the public key can be decrypted only with the private key, and data that is signed with the private key can be verified only with the public key. The public key can be made available to anyone; it is used for encrypting data to be sent to the keeper of the private key. Public-key cryptographic algorithms are also known as asymmetric algorithms because one key is required to encrypt data, and another key is required to decrypt data [5].

3.1 Security on E-mail System

The most serious security problems on electronic mail are (a) cryptanalysis attacks (b) key management attacks (c) playback attacks (d) local attacks (e) untrusted partners and traffic analysis.

In such a cryptanalysis attacks, it mainly targets on having weakness in the cryptography. In the implementation of this system Number Theory Research Unit (NTRU) public key cryptosystem (PKCS) is applied for the intention to have a secure email. Because of NTRU security levels based on the parameters values, and the operation of convolution polynomial rings, the system becomes more secure than other PKCS system. As security problems are important for any email system, it needs to be more secure and endure on various attacks.

In this system, NTRU as well as Hash function are applied for confidential and integrity services. NRTU confirms its cryptography and delivers encryption and decryption and authentication at speeds of multiple time faster than other PKCS (e.g RSA) by applying the system with NTRU and SHA-1 algorithm can accomplish email to be secure from some attacks.

3.2 Number Theory Research Unit (NTRU)

NTRU is a relatively new, ring based cryptosystem that is claimed to be more efficient than the conventional public key algorithms such as RSA. The NTRU algorithm uses a mixing system based on polynomial algebra and reduction modulo two numbers p and q. Its validity depends on elementary probability theory. The reason of the security of NTRU is difficulty of finding extremely short vectors for most lattices.

3.3 NTRU Algorithm

The NTRU algorithm is officially described in. It depends on 3 integer parameters (N, p, q), where N is a prime integer, p and q are relatively prime integers and q is larger than p.

NTRU uses polynomial addition and multiplication in the ring $R = Z[x] / (x^N - 1)$. Any polynomial f in R is written as a vector

$$f = \sum_{i=0}^{N-1} F_i x^i = [F_0, F_1, \ldots, F_{N-1}]$$

In the final step of decryption, the coefficients of polynomials are reduced modulo p. First select two small polynomials f and g (A small polynomial is one in which all the coefficients are either 0,-1, or 1). Select $d_f < n-1/2$ and make d_f coefficients of f to 1 and d_f -1 coefficients of f to -1 and the rest to 0. Similarly selects d_g such that $d_g < n-1/2$ and make d_g coefficients of g to 1 and d_g coefficients of g to -1 and the rest to 0.f and g must be private.

3.4 Key Creation

1. Compute inverses of f mod q = f_q and inverse of f mod p = f_p with the property that f. $f_p = 1$ mod p and f. $f_q = 1$ mod q.
2. Compute the public key $h=p^*.f_q^*g$ mod q

   Public key polynomial = h

   Private key polynomial= {f, f_p}

3.5 Encryption

1. Select a message m and put it in the form of a polynomial m with the coefficient between –p/2 and p/2.

2. Pick a random small polynomial r with coefficient +1,-1,or 0 such that r(1)=0
3. Encrypt the message m as e = r * h +m (mod q).

3.6 Decryption

1. Upon receiving the ciphered text e, compute a =f*e (mod q)
2. Express the coefficients of a in the range -q/2 to q/2
3. Compute b=a*f_p mod p
4. Original message m=b

3.7 Secure Hash Algorithm (SHA-1)

SHA-1 proposed by NIST as a message digest function is the version of SHA with a 160-bits message digest. It takes a message of length at most 2^{64}bits. If the length of a message is equal to greater than 2^{64} bits, it will not be processed by SAH-1. SHA-1 is a little slower to execute and presumably more secure because it produces a 160 bits digest as opposed to the128 bits.

4. Implementation of the System

This system is implemented using C# 2010 programming language. In this system, e-mail security is implemented with NTRU public key cryptosystem. This process has two phases: the encryption and the decryption.

4.1 Encryption Process of Sender Side

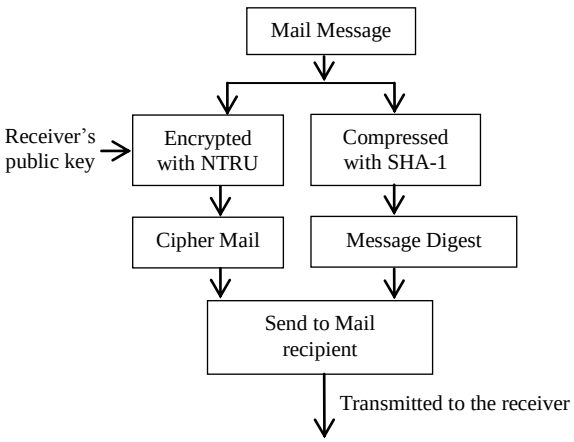

Figure 2. Encryption Process of Sender Side

Figure 1 shows Encryption process of sender side. In this process firstly users need to register first to enter the email system. Admin user can view the list of the registered users and then mail sender's encrypts mail message contents by using NTRU cryptographic algorithm with receiver's public key. Public key can be generally received from public key announcement or public key distribution. Thirdly for ensure message integrity sender uses SHA-1 cryptographic Hash function to produce hash code from the original message and finally Then, cipher mail and message digest are sent to the mail recipient side through over insure channel.

4.1.2 Decryption Process of Receiver Side

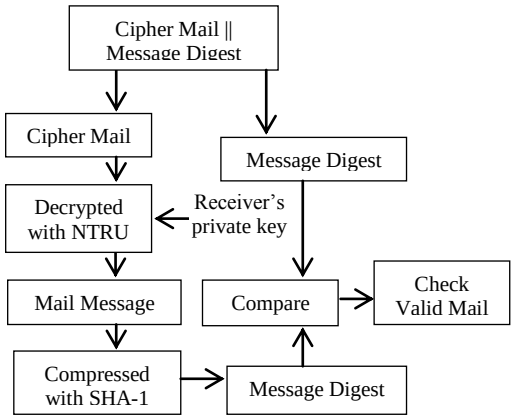

Figure 2. Decryption Process of Receiver Side

Figure 2 shows Decryption process of receiver side.In the receiver side, E-mail recipient needs login to enter the mail system and Recipient can check the received mail and open the mail. The received cipher mail is then decrypted by NTRU algorithm with his own private key. The recipient then hashed the original mail message by using SHA-1 hash function and the two hash codes, one from the sender and the other from calculated hash codes, are compared. Receiver can ensure that the receive mail is a valid
mail if the two hash codes are same, otherwise it is an invalid mail.

4.2 User Interface Form

User interface forms for the implementation of this system are described with their respective processes. E-mail user's needs to login to precede the e-mail system. New users are needed to register to enter the e-mail system. User's needs to fill up correct username and passwords for valid login. Login form for the mail user system is shown in Figure 3.

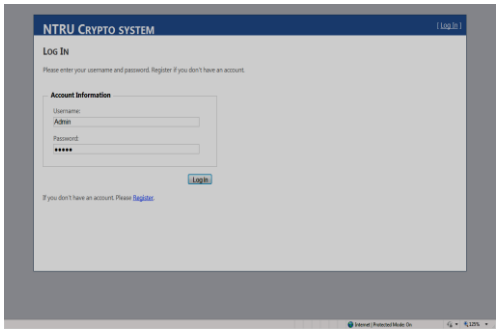

Figure 3. Login Form

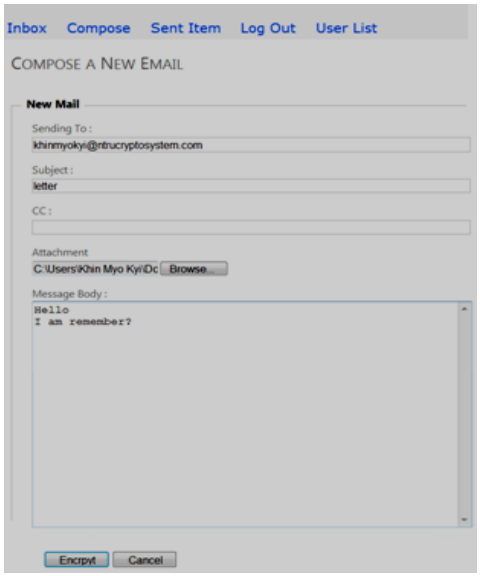

Figure 4. Email Form

The e-mail form is shown in Figure 4. In this form user needs to fill up the required fields. The message is written then encryption process is performed with NTRU cryptosystem for the confidentiality of mail message.

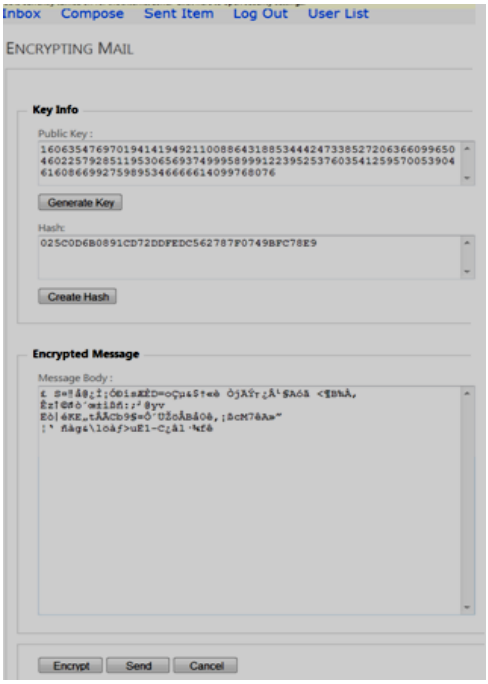

Figure 5. Encrypted Mail

The encrypted mail form is shown in Figure 5. The mail is encrypted with receiver's public key. The original mail message is hashed with SHA-1. After having cipher mail and message digest, the mail user can send the mail through insecure channel providing confidentiality and integrity services.

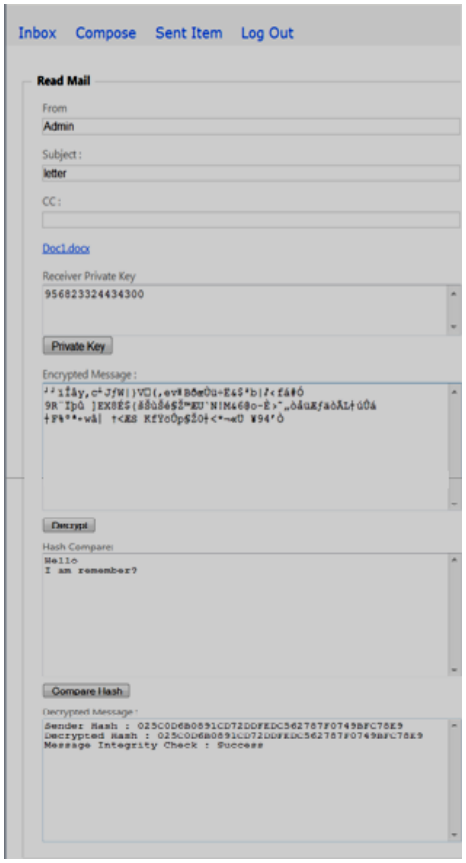

Figure 6. Decrypted Mail

The decrypted mail form is shown in Figure 6. The recipient needs to login first for checking e-mail. He can check received mails in his inbox. The received cipher mail is then decrypted with his own private key by NTRU cryptosystem. The original mail is then hashed with SHA-1 to get message digest. The mail recipient can check the valid of e-mail message that he received by comparing the two hash codes. If the mail is not modified, the integrity checking is success and he can accept the valid mail.

5. Conclusion

As the Information Communication Technology is improving a lot, the host computers in any location communicate each other by sending and receiving email messages over the network. NTRU public key cryptosystem based on encryption standards are applied for email security of the system. NTRU is suitable for faster data transfer rate, low power consumption, and lesser resources need rather than other Public Key Cryptosystem and NTRU meets lesser resources need for the major need of insecure network. In this email security system is not encrypted and decrypted images, audio, video files, attached files and it is only used for mail message files.

Mail messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key. Adding a compression feature (SHA-1) also provided the integrity of the mail system. The mail messages are not zipped in this e-mail security system. In this email security system, only mail message confidentiality and integrity are provided for the mail users. This system can further be extended to achieve other cryptographic security goals concerns with authentication and non-repudiation with secure public key cryptosystem.

References

[1] J.Jun, H. Chen, "A novel mutual authentication and key agreement protocol based on NTRU cryptography for wireless communications", Journal of Zhejiang University Science (JZUS), ISSN 1009-3095, Vo1.6A, Issue 5, p.399-4o4,2005

[2] Mustafa DULGERLER[1] M.SARISAKAL[2], "A Secure Email Application using the Elgamal Algorithm

[3] M.Liskov, R.Rivest, and D.Wagner, "Tweakable Block Ciphers", Crypto 2002 PDF

[4] R. Ricest, "Email encryption using AES"

[5] Wei Ren, NTRU Cryptography Public Key Cryptosystem, Department of Electrical and Computer Engineering University of Nevada, Las Vegas

[6] W.Stallings, "Cryptography & Network Security, Principles and Practices", Fourth Edition, Prentic Hall, 2006, ISBN 81-7758-774-9.