ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

An Efficient Scheme for Message Encryption based on Public Key Crypto System

Venkateswarlu Sunkari[1], S Kranthi Kumar[2], Ato Daniel Abebe[3], M Ananth[4]

[1]Assistant Professor, Centre for ITSC, Addis Ababa Institute of Technology, Addis Ababa, Ethopia

[2] Data Specialist, GBS, IBM India Pvt Ltd, Hyderabad, India

[3] HOD, Centre for ITSC, Addis Ababa Institute of Technology, Addis Ababa, Ethopia

[4]Research Scholar, GITAM University, Visakhapatnam, AP, India.

ABSTRACT: Security is a problem that is more sensitive during a message transmission attributable to the open nature and lack of morality in humans. In order to produce security, information-hiding techniques are proposed. To confuse the attacker or offender of a network by obfuscating message content could be a technique for information hiding. It involves concealing the key text inside the cheating text. If the cheating text is intercepted with security algorithms, the key text should still be undiscovered. In this paper, a NEW message encryption scheme is proposed using cheating text. The sender embeds an evident message in another plain text called Cheating Text. The positions of the characters of the plain text in the Cheating Text are stored in an Index File (IF).This file is encrypted using N-th degree truncated polynomial ring (NTRU) schema and sent beside with the Cheating Text. The receiver once received proceeds to decrypt the IF table and get back the original message from the received cheating text. While Decryption, Authentication is achieved by hashing the plaintext at the sender's side using a Modified Message Digest algorithm and verified at the receivers end.

KEYWORDS: Secret message, Cheating text, NTRU (N-th degree truncated polynomial ring unit), Security, Encryption, Decryption.

I. INTRODUCTION

Instant messaging (IM) is a real-time communication service, which allows a user to send a message, usually based on text, to other users. Nowadays we depend more and more on information from the Internet, and are increasingly not satisfied with accessing the Internet using personal computers or office workstations. Hence, accessing the Internet by portable and wireless devices has been becoming popular. Now a days along with the mobile devices, the security attacks also getting popular.

Security is a vital part of any Message Transmission Systems [1], particularly valuable data like holding bank account, personal group action and et. al. The threats from unauthorized party is growing apace and conjointly increasing in technical sophistication, thereby requiring a depth of defense to safeguard Message transmission [2], against the risks they present with the attacks they deliver.

In order to provide security, so many message encryption systems are developed and implemented [1,3]. However, existing Message encryption schemes require that the total message be encrypted. It leads to increase in the computational cost of message.

In this paper, a new message encryption scheme is proposed using cheating text. The sender embeds an evident message in another plain text called Cheating Text. The positions of the characters of the plain text in the Cheating Text are stored in an Index File (IF).This file is encrypted using N-th degree truncated polynomial ring (NTRU) schema and sent beside with the Cheating Text. The receiver once received proceeds to decrypt the IF table and get

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

back the original message from the received cheating text. While Decryption, Authentication is achieved by hashing the plaintext at the sender's side using a Modified Message Digest algorithm and verified at the receivers end.

II. RELATED WORK

In public key cryptography each user or the device participating in the communication generally have a pair of keys, a public key and a personal key, and a collection of operations associated with the keys to do the scientific discipline operations. Only the particular user knows the private key whereas the general public secrets distributed to any or all users participating in the communication.

Some public key algorithm could require a collection of predefined constants to be better known by all the devices participating in the communication. NTRU associated RSA area unit an example of such public key cryptosystems. in contrast to private key crypto's, that doesn't require any sharing of secret key between the communication parties, the general public key crypto's area unit a lot of slower than the private key crypto's. Normally hash functions suffer from varied sorts of collisions.

MD5 [4] is a hash algorithm to prepare a message digest for a given plaintext. However, this suffers from Wang's collision attack. MD5 algorithm is modified to sustain the Wang's collision attack. The thought is to use 64 -bit-chaining variables instead of 32-bit chaining variables. In this following algorithm padding bits means message is "padded" (extended) so that its length (in bits) is congruent to 448 modulo 512[6].

RSA could be a Public key algorithm fictitious in 1977 by Rivest, Shamir, and Adelman. RSA [5] supports coding and Digital Signatures, most widely used public key algorithm and gets its security from integer factoring drawback. Relatively easy to understand and implement, RSA gets its security from factorization problem. Difficulty of factoring large numbers is the basis of security of RSA. Over one thousand bits long numbers area unit used. In this paper, NTRU performance is compared with that of RSA.

Unlike RSA, NTRU [7] is not widely used, and in fact, the NTRU cryptosystem needed changes early on to improve its security by addressing weaknesses and performance. However, today NTRU is recognized as faster than the widely used RSA algorithm. Comparing NTRU to other cryptosystems like RSA and ECC shows that NTRU, at a high security level, is much faster than RSA (around five orders of magnitude) and ECC (around three orders of magnitude). NTRU may be more resistant over time to attack than RSA because NTRU is constructed in what crypto researchers call a "lattice" framework. NTRU [8,9] consists of two algorithms: NTRU Encrypt for public-key encryption and NTRU Sign for digital signatures.

III. NTRU CRYPTO SYSTEM

The NTRU public key cryptosystem was developed in 1996 at Brown University by three mathematicians J. Hoffstein, J.Pipher and J.H. Silverman. 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. NTRU has three integer parameters: N, p, q. N represents the degree of the polynomials at most N-1; p is smaller than q. p and q is small module used to reduce the coefficients of the polynomials. They do not have common divisor. We briefly describe the NTRU algorithm as follows.

A. Key generation

We have to choose two random polynomials x and y in the ring with the restriction that their coefficients are small, usually in {-1, 0, 1}. We import another symbol here: $Z(a_1, a_2)$, which means a set of polynomials with a1 coefficients are a_1 , a_2 coefficients are -1 and the rest are 0.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Usually we choose x from $Z_x(a_x, ax\text{-}1)$ and g from $Z_y(a_y, a_{y-1})$. Then we compute x_p (the inverse of x modulo p) and x_q (the inverse of x modulo q) with the property that

$$x * x_p = 1 \pmod{p} \text{ and}$$
$$x * x_q = 1 \pmod{q}.$$

If x does not have these inverses, another x should be chosen. The pair of polynomials x and x_p should be kept as the private key, and the public key K can be computed by

$$K = p\, x_q * y \pmod{q}.$$

Both x and x_p are used for private key and K is used for public key.

B. Encryption

The message to be sent can be put into a form of a polynomial $m \in Z_m(a_m, a_m)$ whose degree is at most N-1. Then we randomly choose a blinding polynomial $r \in Z_r(a_r, a_r)$ in the ring. So the encrypted message e should be computed by

$$e = r*K + m \pmod{q}.$$

C. Decryption

First, use a part of the private key f to compute Polynomial $i = x*e \pmod{q}$, then $j = i \pmod{p}$, and then we use the other part of the private key x_p to compute polynomial

$$c = x_p * j \pmod{p}.$$

If this procedure is successful, 'c' will be the original message m. Actually, for appropriate parameter values, this probability is extremely high.

IV. PROPOSED SYSTEM

In the proposed message crypto System, the secret message is embed into another plain text called cheating text. The position of the each character of the cheating text is told in a table called character position table. Another table called Index File (IF) is generated from character positions table for the characters of the original message. The IF is encrypted with NTRU crypto system for better performance, which was mention in section-III. By applying hashing mechanism, hash value was generated for secret message. Now, sender sends the cheating text along with the encrypted IF and the hash value of the secret message. The receiver will decrypt the IF and gets back the secret message from the cheating text using IF.

After decryption, hash value is generated for secret message. Now, generated hash value is compared with existing hash value. If both are equal, message is authenticated. The algorithms for encryption are described below:

Step 1: Take the secret message as input value.
Step 2: Take the meaning full cheating text.
Step 3: Embed the secret message into cheating text.
Step 4: Verify the cheating text, all the secret message was existed in the cheating text or not. If existed got to Step 5 otherwise go to Step 3.
Step 5: Generate the Character Position Table to the cheating text.
Step 5: Generate the IF based on character position file.
Step 6: Encrypt the IF with the NTRU crypto scheme.
Step 7: Generate the hash value to the IF using MD5.
Step 8: Encrypt the cheating text and IF hashes using NTRU.
Step 9: Send the compressed results data to the receiver.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

The original message is embedded in a meaningful cheating text. The positions of the characters of the plain text in the cheating text are stored as Index File (RIF). This file is encrypted and sent along with the cheating text and hash value of the original message in the zipped format like Pretty good policy.

To get the secret message at receiver side, we just reverse the direction of the encrypting process, generate the character position table again, and then use the data in the IF to find out the corresponding character. Algorithm for Decryption is described below:
Step 1: Decrypt using NTRU using session key exchanges and then decompress the hash value and the index file.
Step 2: Generate the Hash value of the secret message for finding the correct text. If hash value matched with the received hash value, go to S3. Otherwise, select one more cheating text.
Step 3: Generate the Character Position Table with the help of Cheating text.
Step 4: If the correct cheating text found decrypt the IF.
Step 5: According to the position record in the RIF, we find out the corresponding characters in the Character Position Table. Finally, we will get the real secret message.

V. PERFORMANCE

The NTRU crypto system is a new public key cryptography approved in 2009. NTRU cryptosystem is faster and provide stronger security than other traditional cryptosystems. NTRU algorithm performed very well on the mobile devices and there were no negative effects on the mobile devices‟ performance due to the minor required for the key generation. NTRU does not require high computing power, which makes it the best alternatives for mobile devices with providing either it or more security facility. Here, the performance of proposed scheme i.e., NTRU is compared with RSA and ECC.

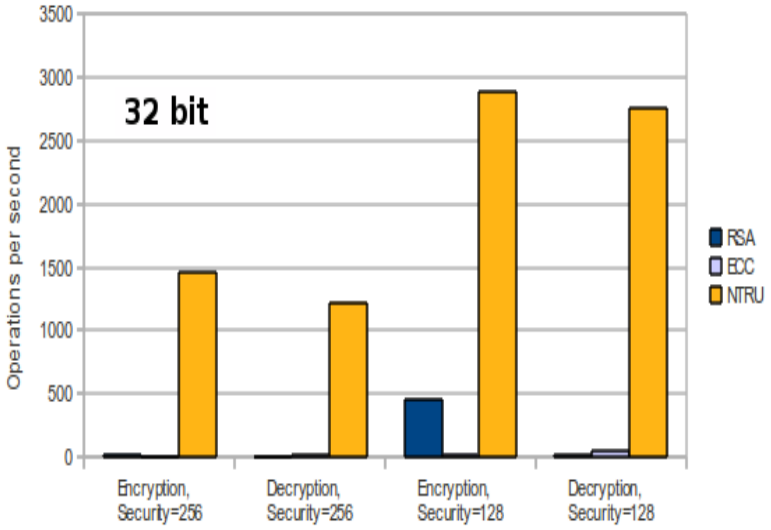

Figure 1: Performance of 32-bit processor

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

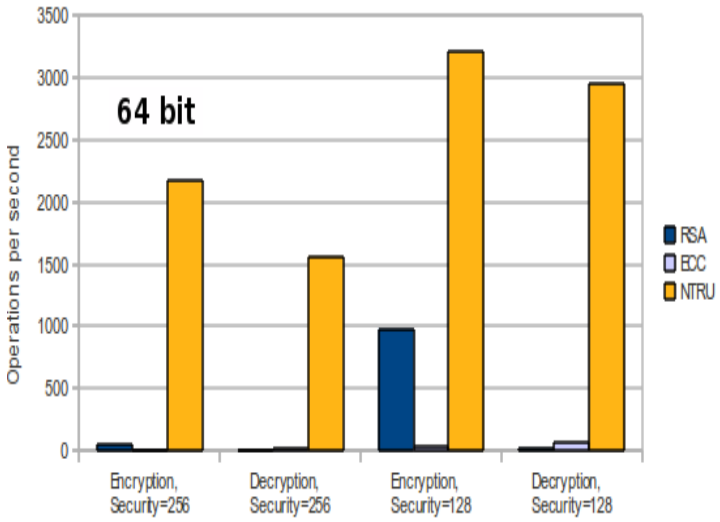

Figure 2: Performance of 64-bit processor

Figure 1 and 2 specifies the performance of various bit processors. The above figure specifies that NTRU out performs when compared with RSA and ECC while encryption security and decryption security. NTRU is significantly faster than other public-key cryptosystems.

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. NTRU 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 as shown in above table. It is the smallest public key crypto available on market.

VI. CONCLUSION

In this paper, a new message encryption scheme is proposed using cheating text. The sender embeds an evident message in another plain text called Cheating Text. The positions of the characters of the plain text in the Cheating Text are stored in an Index File (IF).This file is encrypted using N-th degree truncated polynomial ring (NTRU) schema and sent beside with the Cheating Text. The receiver once received proceeds to decrypt the IF table and get back the original message from the received cheating text. While Decryption, Authentication is achieved by hashing the plaintext at the sender's side using a Modified Message Digest algorithm and verified at the receivers end.

REFERENCES

[1] 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 securitystrategy", International Journal of the Physical Sciences Vol. 6(4), pp. 930-938, 18 February 2011.
[2] H. J. Highland, "Data encryption: a nonmathematical approach-Part 5," Journal of computer and Security, pp.93-97, 1995.
[3] Priya Dhawan, "Performance Comparison: Security Design Choices", Microsoft Developer Network, October 2002. http://msdn2.microsoft.com/enus/library/ms978415.aspx
[4] Ch. Rupa and P. S. Avadhani," An Improved Method to Reduce the Occurrence of Collision Attack on Hash Function", Int. J. computing mathematical applications, vol2, No1-2, pp.121-131, 2008.
[5] Aamer Nadeem et al, "A Performance Comparison of Data Encryption Algorithms", IEEE information and communication, pp .84-89, 2005.
[6] H. Dobbertin, ―Cryptanalysis of MD5 Compress, proc. of Eurocrypt- 96, 1996.
[7]http://features.techworld.com/security/3275990/ntruencrypt -the-fastest-public-key-algorithm-youve-never-heard-of/
[8] Carlos Cid,"Recent developments in Cryptographic hash Functions: Security implications and future directions", Information Security Technical Report ,vol.26, pp.100-107, 2006.
[9] R Weis and S Lucks, ―Cryptographic Hash Functions-Recent Results on Cryptanalysis and their Implications on System Security, 5th System Administration and Network Engineering Conference, pp 15-19, 2006.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

BIOGRAPHY

Venkateswarlu Sunkari is an Assistant Professor in the Centre for Information Technology and Scientific Computing under the School of Electrical and Computer Engineering, Addis Ababa Institute of Technology, Addis Ababa University, Ethiopia. His research interests are Software Engineering, Computer Networks, Cryptography and Network Security, Cloud Computing, Mobile Computing etc.

S Kranthi Kumar is Data Specialist, GBS, IBM India Pvt Ltd, Hyderabad. His research interests are Computer Networks, Cryptography and Network Security, Data Mining , Mobile & Cloud Computing etc.

Ato Daniel Abebe is Head of the Department in the Centre for Information Technology and Scientific Computing under the School of Electrical and Computer Engineering, Addis Ababa Institute of Technology, Addis Ababa University, Ethiopia. His research interests are Computer Networks, Cryptography and Network Security, Cloud Computing etc.

M Ananth is Research Scholar in Department of Computer Science and Engineering, GITAM University, Visakhapatnam, AP, India. His research interests are Computer Networks, Network Security & Cryptography, Cloud Computing etc.