Dual Encryption Schema With Cheating Text and NTRU

Jagadeeshbabu.G[#1], Rakesh Nayak[#2],

#1 Student, Sri Vasavi Engineering College, TaddepalliGudem, Andhra Pradesh,

#2 Assoc. Professor, Department of IT, Sri Vasavi Engineering College, TaddepalliGudem, Andhra Pradesh ,

Abstract: Shared data systems have grown in numbers and hence they are susceptible to many security challenges. The sender embeds a plain message in another plain text called Cheating Text. The positions of the characters of the plain text in the cheating text are stored in a Real Message Index File (RIF).This file is encrypted using N^{th} degree truncated polynomial ring (NTRU) scheme and sent along with the cheating text. The receiver once received, proceeds to decrypt the RIF table and gets back the original message from the received cheating text. Authentication to decrypt is achieved by NTRU key exchanges prior to session initiation at both senders and receivers side along with the MD5 hash of the RIF. An NTRU 263-bit encryption key, has cryptographic strength equivalent to renowned powerful 1024-bit RSA key. We propose to replace any secure Scheme with a more robust NTRU crypto system.

Keywords— NTRU,MD5,RIF,CPT.

I INTRODUCTION

Message Encryption schemes currently being used encrypt the total message that needs to be transmitted. This paper encrypts that part of the message which is confidential rather than the total message using the concept of cheating text. Cheating text is any kind of meaningful text which is a metamorphosis of hidden writing. The concept of cheating text comes from Steganography, in particular data hiding[1]. Plain text message is inserted into another text called the cheating text and the positions of the characters of the plain text are stored in another file called real message index table(RIF). Now the RIF table is hashed using MD5 which serves as the primary cipher coating. The entire contents(cheating text + hashed RIF table) are then encrypted using an N^{th} token polynomial cipher which acts as the second coating thus justifying dual encryption schema. One interesting feature of this kind of an approach is the implementation of three layered content protection procedures involving steganography using cheating text, RIF hashing using MD5 and finally entire content ciphering using NTRU suggests that finally obtained ciphered content is so robust and secure that it has potential to be compared with any 1024-bit ciphers such as RSA or ECC(Elliptic Curve).

The main theme of the cryptography is to transform a message such that it is incomprehensive to an unauthorized reader. This is an overt secret writing; that is, the transformed result is obviously recognizable as a secret message[1]. On the other hand, steganography is one kind of covert secret message or hidden writing. Its aim is to conceal the very existence of a message-to send a secret message without incurring suspicion.

In this paper, A hash value of the positional indexes(RIF) of characters pertaining to cheating text containing the plain text is hashed using MD5 and then cheating text and RIF combo is ciphered using the NTRU Algorithm in order to provide authentication at both the ends based on key exchanges of both the sender and reciever. The NTRU is a public-key algorithm competes with RSA and elliptic curve. The encrypted file is sent to the receiver along with the cheating text and the hash value of the plain text. The receiver decrypts the RIF file and obtains the original message using the cheating text. The hash value is re-calculated at the receiver’s end to verify the message and hence authentication is achieved.

II RELATED WORK

In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations.

Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. NTRU and RSA are an example of such public key crypto systems. Unlike private key crypto's, that does not require any sharing of secret key between the communicating parties, the public key crypto's are much slower than the private key crypto's.

Normally hash functions suffer from various types of collisions. MD5[2] 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 idea 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[3].

RSA is a Public key algorithm invented in 1977 by Rivest, Shamir, and Adelman. RSA[4] supports Encryption and Digital Signatures ,most widely used public key algorithm and gets its security from integer factorization problem. 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 1000 bits long numbers are used. In this paper, NTRU performance is compared with that of RSA.

III ABOUT NTRU

Unlike RSA, NTRU[6] is not widely used, and in fact the NTRU cryptosystem needed changes early on to improve its security by addressing weaknesses and performance. But 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] consists of two algorithms: NTRU Encrypt for public-key encryption and NTRU Sign for digital signatures. NTRU is lattice-based and not known to be breakable even with quantum computers. Commonly used cryptosystems like RSA or ECC, on the other hand, will be broken if and when quantum computers become available. In addition, NTRU is significantly faster than other public-key cryptosystems.

III PROPOSED SCHEME

In the proposed crypto System the message is embedded into another 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 the RIF is generated from character positions table (CPT) for the characters of the original message. The RIF is encrypted with any public key crypto system, we propose to use NTRU for better performance. The cheating text along with the encrypted RIF and the hash value of the original message are sent. The receiver will decrypt the RIF and gets back the original message from the cheating text using RIF.

This received original message is again hashed and compared with the received hash value. If they are equal the original text is authenticated. The algorithm for encryption and decryption of the process is explained below.

Algorithm:
Step 1: Take the input value as Plain text.
Step 2: Take the meaning full cheating text.
Step 3: Verify the cheating text, all the plaintext was existed in the cheating text or not. If existed got to Step 4 otherwise go to Step 2.
Step 4: Generate the CPT to the cheating text.
Step 5: Generate the RIF (real message Index File)
Step 6: Encrypt the RIF with the any secure Scheme.
Step 7: Generate the hash value to the RIF using MD5.
Step 8:Encrypt the cheating text and RIF hashes using NTRU.
Step 9: Send the compressed results data to the receiver.

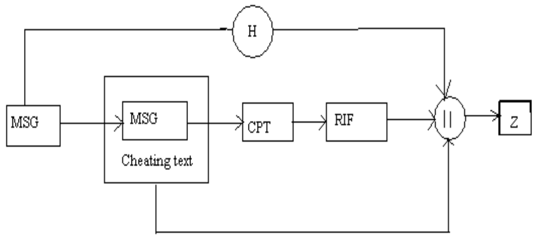

FIG1: Protection Scheme with NTRU

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 Real Message 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 as shown in Fig 1.

In the following we show the decrypting process of the Improved Document Protection Scheme. We just reverse the direction of the encrypting process and generate the CPT again and then use the data in the RIF to find out the corresponding character.

Algorithm:

Step 1: Decrypt using NTRU using session key exchanges and then decompress the hash value and the real message index file.
Step 2: Generate the Hash value of the plain text 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 CPT with the help of Cheating text.
Step 4: If the correct cheating text found decrypt the RIF.
Step 5: According to the position record in the RIF, we find out the corresponding characters in the CPT. Finally, we will get the real message.

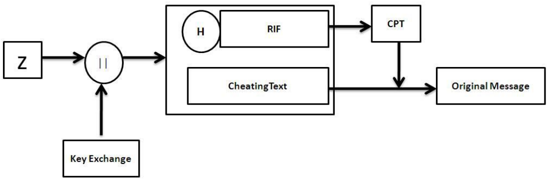

FIG2:Decryption

.V CONCLUSION

A message encryption scheme based on cheating text is proposed. For message encryption NTRU is proposed. The scheme is cost effective because only a index table called RIF file is hashed and sent to the receiver along with the cheating text in which the original message is embedded. The size of data being passed to hashing algorithms, as well to cryptography techniques, is also significant. The original message can be retrieved from the RIF file table and the cheating text. The hash value is re-calculated at the receiver's end to verify the message and hence authentication is achieved. This scheme can be applied for authentication like security in data bases.

VI REFERENCES

[1] H. J. Highland, —Data encryption: a non-mathematical approach-Part 5, Journal of computer and Security, pp.93-97, 1995.

[2] 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.

[3] H. Dobbertin, —*Cryptanalysis of MD5 Compress*, proc. of Eurocrypt ‗96, 1996.

[4] Aamer Nadeem et al, *"A Performance Comparison of Data Encryption Algorithms"*, IEEE information and communication, pp .84-89, 2005.

[5] Priya Dhawan.,*"Performance Comparison: Security Design Choices*‖, Microsoft Developer NetworkOctober2002.http://msdn2.microsoft.com/en us/ library/ms978415 .aspx

[6]http://features.techworld.com/security/3275990/ntruencrypt-the-fastest-public-key-algorithm-youve-never-heard-of/

[7] 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.

[8] Carlos Cid,"Recent developments in Cryptographic hash Functions: Security implications and future directions", Information Security Technical Report ,vol.26, pp.100-107, 2006.