To Secure and Compress the Message on Local Area Network

Gagandeep Shahi
Research Scholar
Department of CSE,
RIMT institutes

Charanjit Singh
Assistant Professor
Department of CSE,
RIMT institutes

ABSTRACT

In the modern world data security is an essential part to inviolability of the crucial facts. Now the days we deal with digital world to perform tasks such as online cash withdraw from bank, cash submission to bank and online payment receive from clients, online payments to our sellers etc. With the ease to get internet connection, we can say that e-business getting at the peak in these days. In these days Common men showing full interest in e-commerce and e-business. They are transmitting their exigence information in the form of conspicuous passwords, decisive data and esteemed information on the insecure network. To prevent these significant facts data security must be there to target such as confidentiality of facts, integrity of facts and availability facts. Fulfillment of these targets done by the Secret writing also called encryption. If we encrypt the data at sender side then we have to decrypt it at receiver side to make that data in original form, this process is called cryptography. In this paper we will discuss the techniques of the cryptography through two network models named as client server and peer to peer. It also seems that if we implement public key cryptography technique with compression using Peer to Peer on Local area network then can secure and fast the communication of the organizations.

General Terms

Cryptography, Compression, Public key, Private Key

Keywords

RSA, NTRU, Digital Signature, P2P, LAN

1. INTRODUCTION

In this modern winged growth of digital interchange and electronic information barter, almost all from us communicate through cyber space without think a moment about security. We all send a lot of personal and crucial information through cyberspace. In short information is plain for web thugs. Anything at all we send through web is unprotected. For assist this shaky information we use the cryptography or secrete writing on our computer network. We all know computer network is a bunch of two or more computer nodes linked with some kind of media may be wired or wireless to interchange the information. So to protect the authoritative data we apply the cryptography on one of these architectures. Cryptography is an area of computer science which is developed to provide security for the senders and receivers to transmit and receive confidential data through an insecure channel by a means of process called Encryption/ Decryption[9]. It seems that we can use compression with encryption to fast transmission. Compression and Encryption are encoding techniques with difference of motive one reduce the size another hide the sensitive information. Peer to peer is an approach where according to the situation two parties act like client as well as server.

1.1 Concept of Cryptography

Cryptography is a mathematical, scientific as well as artistic approach to alter the chief information into inscribe format so that it is only understand by sender and receiver of data for security purpose. In cryptography sender shroud the original information by transposition or substitution method called encryption. Original Message format also called the plain text and inscribe format called cipher text Shown in the Fig 1.

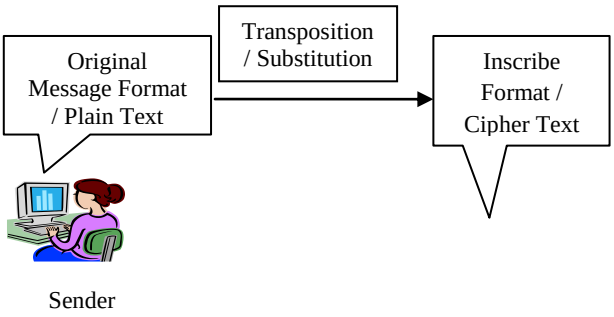

Figure 1:- Encryption process

On the other hand when inscribe format turn back into the original message format at the receiver end this whole process called the decryption Shown in Fig 2

.

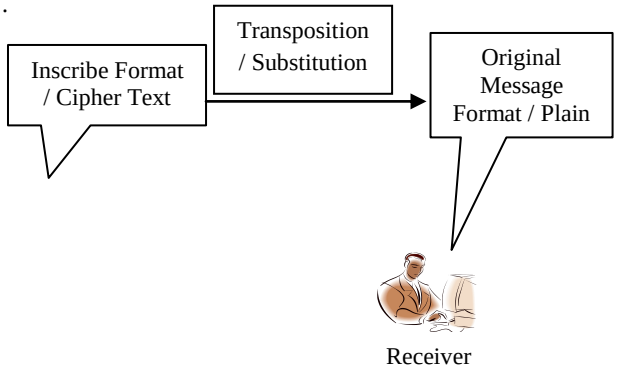

Figure 2:- Decryption process

1.2 Objectives of Cryptography

1.2.1 Encryption/Decryption: - Primary goal of Cryptography system is Encryption/Decryption of information. Encryption changes the original pattern of data into unreadable form so that exigence information never understands by the unauthorized software or node. Decryption is the vice versa process of Encryption. In the decryption

authorized software or node convert back the unreadable format to original format of data to understand the message send by the sender.

1.2.2 Authenticity: - Authenticity is also an important goal of cryptography. It ensures that data must be decrypt by authenticated node or a person who have the valid key to decrypt the data. If any intruder trying to decrypt it then he should unable to understand and read it.

1.2.3 Integrity: - When data transmit over the network integrity is a very important Objective of cryptography. It ensures that data that were sending by sender was not modified during the path to receiver that was selected for transmission. For this purpose the sender create the message hash when this hash receive by receiver he check this with previous hash for confirmation.

1.2.4 Non-Repudiation: - This is very important feature of cryptography. Sender never refuses that he or she never sends the data. For example the cryptography uses the digital signature for this purpose. Receiver matches current signatures with previous one for confirmation of the valid sender.

1.3 Keys used in Cryptography

Types of the cryptography depend upon the way of keys used for Encryption and Decryption. Keys are the methods which we use to encrypt and decrypt the data. There are two types of methods or keys to encrypt and decrypt data are public key and private key. Every node or system must have these two keys in the network.

1.3.1 Private Key: - It is the method that known by sender or receiver himself/herself and also to authenticated person. We can also call it as private or personal key Shown in the Figure 3.

1.3.1 Public Key: - This is the method that can be known by all members of the network.

For example Figure 3 showing that Private Key is only known by the Rose in the network. On the other hand public key is known by all members of network Salman, Jack and Aish.

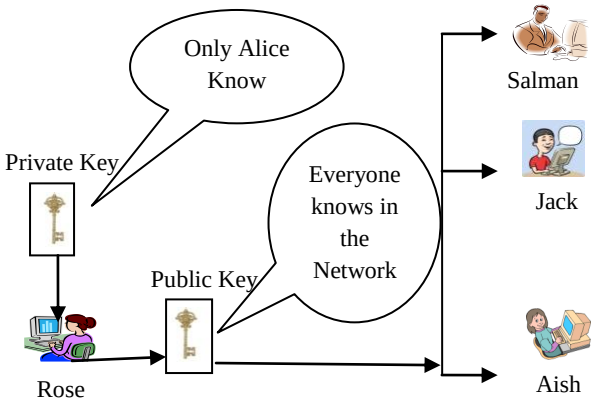

Figure 3:- Showing the Private and Public Key of Alice

1.4 The Cryptography Techniques

1.4.1 Same Key Cryptography: - This Type of cryptography also known as the Private Key cryptography, Personal key Cryptography and Symmetric Key Cryptography etc because in this we use only receiver's Private Key for encryption and decryption of data. Some people call this One key or Single key cryptography technique because we use in this technique only the one key for transposition or substitute the original characters of the message. Figure 4 showing that Rose and Aish sharing the same key that is Private Key of Lucy for Encryption and decryption.

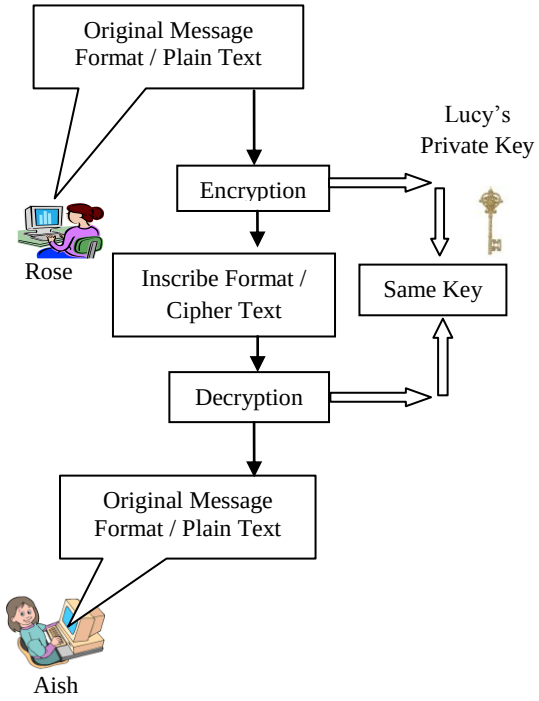

Figure 4:- Showing Lucy's Private Key (Same key) using for Encryption/Decryption

1.4.1.1 Advantages of same key cryptography

This type of cryptography is very simple and sober technique to implement. Users must have to share same key for encryption and decryption, so using this technique we can also encrypt our personal files like hiding data by own password. The major advantages of this type of cryptography approach are that user share different secret key for different party so if it is hacked then only that communication will effect.

1.4.1.2 Disadvantages of same key cryptography

If we want to implement the same key cryptography approach then we must assure that transmission media is fully secured or not because if transmit our sensitive key over the unsecured media intruder can hack our secret key and harm to our sensitive information. Managing too many keys for different parties is very difficult task in same key cryptography. In symmetric key cryptography verification and validation of data cannot be possible due to same key used by sender and receiver that's why it is impossible to know who send the message.

1.4.2 Different Keys Cryptography

Different key cryptography technique is very hot cryptography technique in these days. Same key cryptography has some disadvantages like it need secure transmission media, no verification and validation possible etc. this cryptography technique is vice versa of same key cryptography technique. It has so many names like public key cryptography, Asymmetric key cryptography etc. Different keys Cryptography use two keys Public key of receiver to encrypt the data and Private Key of receiver to decrypt the data. For example Figure 5 showing that if Rose wants to send the message to Aish she will first encrypt the message with Aish's Public Key at the receiver side Lucy decrypt that message with her own Private Key.

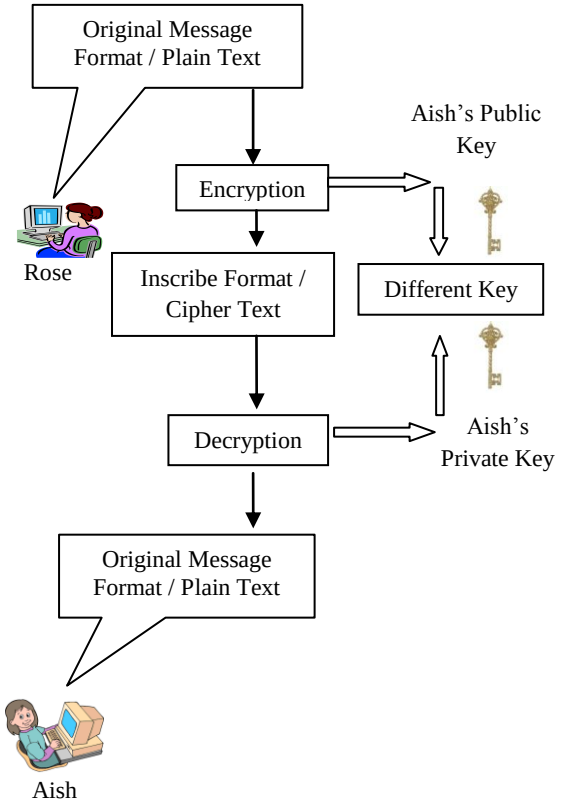

Figure 5:- Showing the Private and Public keys (Different keys) of Aish using for Encryption/Decryption

1.4.2.1 Advantages of Different key cryptography

Major advantage of different key cryptography is that it facilitate to verify, validate and non-repudiation of the data through digital signatures or digital certificates. It uses two keys Public and private. Public key can be known by anyone but private key remain secret of each computer in the network that's why no need for secret key exchange over the network.

1.4.2.2 Disadvantages of Different key cryptography

It depends upon trapdoor computations that are expensive to encrypt and decrypt so these are also slow as compare to same key cryptography. In the public key cryptography key size become large that is the cause of slow encryption and decryption.

1.4.2.3 Applications of different key cryptography

1.4.2.3.1 Digital Signatures

Digital signatures are the unique identifications of the electronic document or the message. It assures that message comes from right person. We create message hash with hash functions and encrypt that hash with sender's private key and create digital signature. This digital signature adds with original document and sends to receiver. At the receiver end receiver also apply the hash function on the original message and create new message hash. Receiver decrypts the Digital Signature of the document by public key of the sender. After this he match new massage hash with decrypted massage hash if both message hashes' not match then there is tempering in message on the way otherwise message is right.

1.4.2.3.2 Digital certificates

Digital certificates are the documents that are signed by the authority centres. Authority centres are third parties who are responsible of security of the network. They are consisting of one or more servers and certify the documents by issuing a signed document called certificate. These certificates assure that document comes from right place without any modification during the way that it follows during the transmission. If receiver received the message with trusted parties certificate then no need to think about security issues in the transmission.

1.4.3 Hash Cryptography

Hash cryptography basically use the fixed length hash functions for encryption and decryption rather than public or private keys. It provides convenience to communication using algorithms. By using this type of cryptography we can also hide our important passwords. It prevents the tempering of the message during its journey on the network.

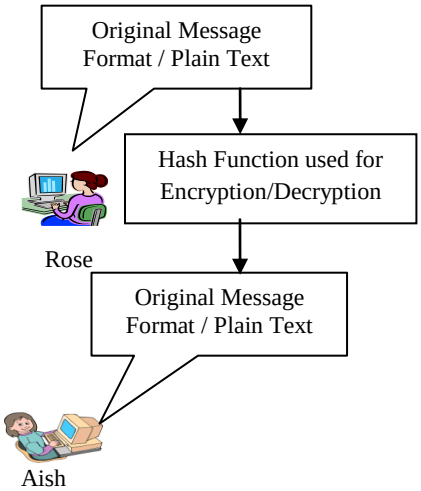

Figure 6:- Showing the hashing

1.5 Different key Cryptography algorithms

1.5.1 RSA (Rivest Shamir Adleman)

RSA is commonly used algorithm of public key cryptography or Different key cryptography because it is very popular approach that is based upon factoring problem. Factoring problem is that in which guessing the factors of large integers are difficult. Algorithm generate and multiplying two prime numbers with some additional operations to obtain Public key and Private Key. Once both key are generated RSA can be use for Encryption/Decryption as well as Digital Signatures. . The security of RSA algorithm depends on the ability of the hacker to factorize number. Although the past work has proven that none of the attacks on RSA cryptosystem were dangerous [11].

1.5.2 NTRU

NTRU is an approach that based upon factoring problem of Polynomials. It is purely lattice based approach. NTRU stands for Nth Degree Truncated Polynomial Ring Unit. In this approach polynomial rings are used to generate public and private keys for Encryption and Decryption. Due to polynomial used in this approach key size used in encryption and decryption always become small as compare to integers factoring based approaches. This algorithm also used for digital signature.
NTRU is actually a parameterized family of cryptosystems; each system is specified by three integer parameters (N, p, q) which represent the maximal degree N-1 for all polynomials in the truncated ring R, a small modulus and a large modulus, respectively, where it is assumed that N is prime, q is always larger than p, and p and q are co-prime; and four sets of polynomials L*f*, L*g*, L*m* and L*r* (a polynomial part of the private key, a polynomial for generation of the public key, the message and a blinding value, respectively),all of degree at most N-1 [7].

1.6 Compression

Compression is a powerful approach that is responsible for proper utilization of system resources or network resources like storage capacity of network and proper transmission media utilization. Data compression, source coding, or bit-rate reduction involves encoding information using fewer bits than the original representation [3]. Compression produces the compact size of the message. It has two techniques lossless and lossy. Lossless is an approach that does not harm the quality of the data normally apply on texts. Lossy compression is an approach that may reduce the quality of the data example of this is image compression.

1.6.1 Simple String Compression Algorithm

It is a lossless compression approach. This approach reduces the size of a byte array into 5 bits. We all know that every character of the string have some ASCII codes American Stand Code for Information Interchange. This ASCII code can be representing in 8-bits. In Simple String compression Algorithm we reduce these 8-bits into 5-bits by removing extra bits.

2. PROBLEM DEFINATION

When we talk about the security of the Local Area network that is the network of an organization with in the campus like colleges, industries etc we always depend upon the Central Security Server to send and receive the messages. Security of the central Server may be weak so that intruder can hack this Central Server and destroy all transmission. Transmission delay can be there due to cartelized approach because if 'A' wants to send message to 'B' then it is not possible to send message directly without authentication of Centralized Server. So there is a need of strong security technique that may not base upon Central Security Server.

3. PERPOSED WORK

It seems that if we implement Public Key cryptography technique with combining compression using Peer to Peer on Local Area Network can solve the problem of dependability on Central Security Server on LAN who is responsible for security of the message. This technique can improve the security of the message as well as fast transmission.

3.1 Peer to Peer Method (P2P)

Peer to peer is an approach in which transmission occur between two nodes directly without using Central Server. Both nodes act like Client and Server according to the situation. Figure 7 showing the transmission between Rose and Aish by excluding Central Server using Peer to Peer.

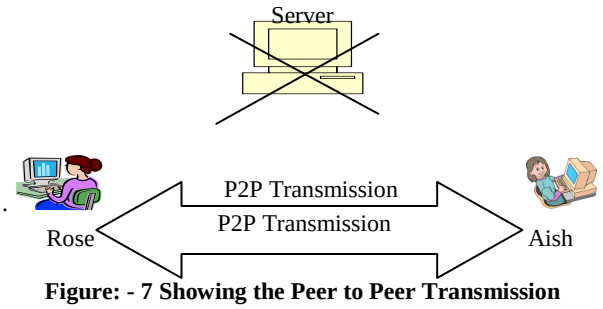

Figure: - 7 Showing the Peer to Peer Transmission

4. METHODOLOGY

We will implement the compression with public key Cryptography by P2P on Local Area Network using JAVA which supports the Network programming. Network programming allows the efficient communication between Network processes. It allows us to writing computer programs that communicate with other program across a computer network. Network program can do lots of work. A simple network Program can obtain information from many computers located all over the world [4]. We will generate a program using network programming that will combine the compression with encryption and will work with peer to peer Principal on the Local Area Network. We will develop application using Simple String Compression Algorithm on two different algorithms of Public key cryptography called RSA and NTRU to secure the message on local Area Network using Peer to Peer and find out the best fit algorithm in this approach. Figure 8 showing the method how applications will combine and extract the Compression and Encryption sender side and receiver side.

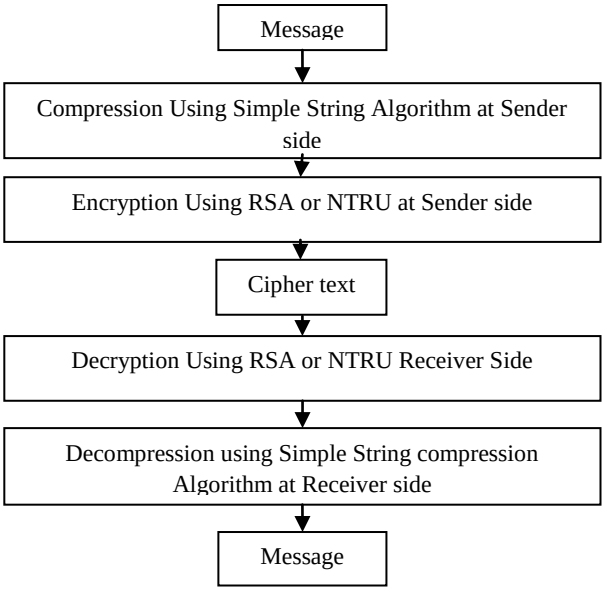

Figure: - 8 Showing the Method to combine Compression and Encryption at Sender side and its reverse on Receiver side.

5. CONCLUSION

In this paper we discuss the Cryptography and Compression. It seems that if we apply the compression with public key cryptography on Local area network using Peer to Peer will improve the security of the message on Network as well as improve the Transmission over the transmission media because message size will be compact. It will be very hard for intruders to attack the message because message will encrypt with Public key cryptography that will use the different keys for encryption and decryption. We can also improve the validity, integrity and non-repudiation of the network using these public key algorithms.

6. ACKNOWLEGEMENT

First of all I want to thank the light of god who guided me throughout the way. I would also like to thanks an Assistant Professor Charnjit Singh for his great efforts of supervising and leading me to accomplish this fine work.

7. REFERENCES

[1] Dr. Qais Faryadi (2013) "Does Data Security Matter? The Case for Cryptography**"** The 2nd International Conference on Computer Science & Computational Mathematics (ICCSCM).

[2] Megha Ojha, Priyank Dubey (2013) "Sharing of Encrypted Information in a Network Using Block Cipher Cryptography" International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1.

[3] Rupinder Singh Brar, Bikramjeet singh (2013) "A Survey on Different Compression Techniques and Bit Reduction Algorithm for Compression of Text/Lossless Data" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 3.

[4] Abhijit A. Sawant, Dr. B. B. Meshram (2013) " Network programming in Java using Socket**"** International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 3, Issue 1, January -February 2013, pp.

[5] Shaik Rabbani, Rakesh Nayak, Dr. J. Pradhan (2013) "An NTRU Scheme for Secure Transaction in Grid Implementation" International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 2.

[6] Pawandeep Singh Aujla, Harneet Arora (2013) "A Secure Account based Mobile Payment Protocol with Public Key Cryptography and Biometric Characteristics" International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.

[7] Raj Kumar, Naveen Kumar, Chandra Sekhar P, Bhargav Nunna, Vinod Kumar B (2012) "International Journal of Computer Science and Network (IJCSN)" Volume 1, Issue 4, August 2012, ISSN 2277-5420.

[8] Sameer Hasan Al-Bakri1, M. L. Mat Kiah, A. A. Zaidan, B. B. Zaidan and Gazi Mahabubul Alam (2012) "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 .

[9] Monika Agrawal, Pradeep Mishra (2012) "A Comparative Survey on Symmetric Key Encryption Techniques" International Journal on Computer Science and Engineering (IJCSE).

[10] A. Medani, A. Gani, O. Zakaria, A. A. Zaidan, B. B. Zaida (2011) "Review of mobile short message service security issues and techniques towards the solution" Scientific Research and Essays Vol. 6(6), pp. 1147-1165.

[11] E.Thumbiraja, G. Ramesh, Dr. R. Umarani (2012) "A Survey on Various Most Common Encryption Techniques" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X

[12] Sachin Upadhyay (2011) "Attack on RSA Cryptosystem" International Journal of Scientific & Engineering Research Volume 2, Issue 9, ISSN 2229-5518

[13] Mohammed Abutaha, Mousa Farajallah, Radwan Tahboub & Mohammad Odeh (2011) "Survey Paper: Cryptography Is The Science Of Information Security" International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (3).