ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

Security through Smart Encryption

Vishi Tomar, Dr. (Prof.) Jayant Shekhar
M.Tech CSE Scholar Swami Vivekanand Subharti University, Meerut
Paper Guide Swami Vivekanand Subharti University, Meerut

Abstract— This paper has a new approach for encryption of text files. It encrypts data at different-different level. First of all ASCII (American Standard Code for Information Interchange) of each character has been taken. Than we check from 2 to no-1, how many digits divide that number than we add that value in our ASCII value and new text file has been created. Value in the binary data of file is divided into variable size blocks called as grids. The bit stream of each grid is taken and bits manipulation read diagonal wise is applied. The key is wrapped up with some public key algorithm say RSA for secret key transposition so that intruder cannot identify. For decryption the reverse grid transposition and private key is required. The included session key is obtained by decrypting the wrapped key with receiver's private key. As we get the text file, a reverse process will be followed and we predict that value that will be added in original ASCII value, after getting original ASCII value, original text file will filling by this process.

Keywords: **Cryptography, Cipher Methodology, Grid Transposition, Circle generation, key wrapping**

I. INTRODUCTION

Today the prominence of internet in day to day life has increased a lot. Various transactions in defense, file transfers in an organization internally requires network security. With the availability of internet, many intruders across the world can access our data. In order to rescue our data from intruders we need CRYPTOGRAPHIC techniques .Cryptography is the science of using mathematics to encrypt and decrypt the data. It enables you to store information and transmit it across insecure network so that it cannot be read anyone except recipient. The same plaintext encrypts to different cipher text with different keys. It depends on the strength of the cryptographic algorithm and the secret of the key. Cryptography is conversion of original data into some modified form of data called cipher. As we know that security is a broad topic. It is concerned with making to sure that no one an unauthorized user cannot read or worse yet, secretly modify messages intended for other receipents.Security problems can be divided into four closely areas: secrecy, authentication, non repudiation and integrity control. Secrecy deals any sender and receiver should be able to understand the content of the transmitted message. Authentication deals having confidence those users and clients identities are correctly known. Non-repudiation deals with signature. Integrity control deals ensuring that data is not modified during transmission. Various algorithms have been proposed till now and each has their merits and demerits. As a result researchers are working in the field of cryptography to enhance the security further. In this paper a new approach is proposed where the source file has been changed and than file is considered as a stream of bits and constructed as various grids. Network security involves the authorization of access to data in a network, which is controlled by the network administrator The technique transforms each grid into encrypted grid by applying bit permutations. The key generated is also wrapped to get encrypted key. The efficiency of this method is that it supports a variable length grid, secure variable length key. Digital Signature is one of the most widely misunderstood terms in the area of computer security. On the sending side, the sender would encrypt the message digest with her private key. The sender must secretly hold the private key at all times.

a. The output of this process is called as the digital signature for this particular message.

b. The sender sends the original message and the digital signature to the receiver.

c. The receiver verifies (decrypts) the digital signature using the sender's public key, which is available very openly. This should give the receiver a message digest, say MD-1.

d. The receiver also computes a fresh message digest on the original message, say MD-2.

e. If MD-1 = MD-2, we achieve both message integrity (message has not been tampered with, because the attacker does not know the sender's private key) and non-repudiation (the message is proven to be sent by the sender, since only she knows the private key corresponding to this public key)

f. After that process file will be converted into grid and bits manipulation will be performed on grid and original file will be achieved.

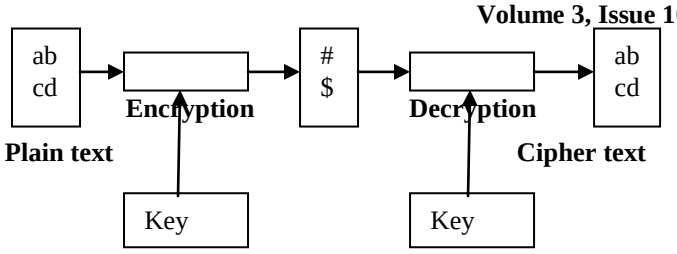
II. SECURITY TECHNIQUES

There are two techniques to implements security goals.
Symmetric key encryption Asymmetric key encryption

1. Symmetric key encryption

It is a class of security techniques that use the same cryptographic key for encryption and decryption of the text. The given figure shows the symmetric key encryption that how the same key will work on encryption and decryption the text.

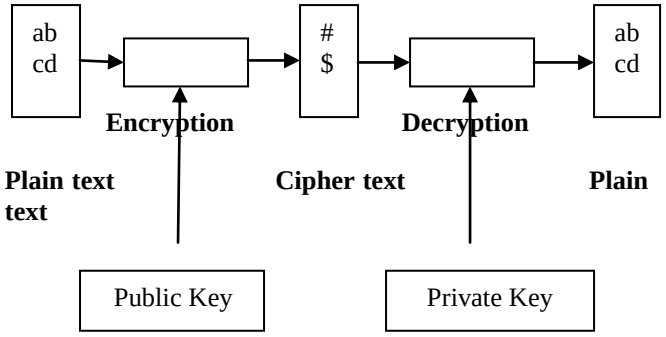
ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014



Symmetric key encryption

2. Asymmetric key encryption

Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.



Asymmetric key encryption

III. NEED OF SECURITY

Security is often viewed as the need to protect one or more the aspects of network operation. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. Security is something that has grown to be a main concern among society. Primary elements of security of any network include security at the sending node, intermediate forwarding node, receiving node, interconnection links and mechanism of transmission or reception at physical and logical level. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. It starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name —i.e. the password— this is sometimes termed one-factor authentication.

IV. DRAWBACKS

1. It will very difficult to manipulate changed grid as character goes beyond the range of readable character and to get back them changed the original file.
2. As that algorithm uses DSA algorithm, at many places communicating with private, public key is not possible. At that stage that algorithm is not possible.
3. Its involves lot of calculates, so it will take lot of time to encrypt and decrypt message
4. As we are working with binary data, so we have to pay extra attention, as to work with binary data is not very feasible.

V. METHODOLOGY

To fulfill the drawbacks now we used the given methodology

Step 1:A binary data (ASCII value of individual character) has been taken from source file

Step 2:Add the certain number in binary value that has been taken by applying a procedure, we will check now many integers come from 2 to (no-1) ASCII value-1 of individual character.

Step 3:A new intermediate file has been getting by calculating new ASCII values.

Step 4: Now we take required size (variable size) grid.

Step 5:Now grid transposition is applied by reading data as various circles starting from the top of the grid to the bottom at various levels (diagonally) and writing it down on left to right and top to bottom.

Step 6:A new grid is generated after transposition

Step 7: The new grid is converted into ASCII sequence and written to another file called encrypted file.

Step 8: Steps 1 to 7 are repeated until the total file is formed into grids and encrypted. Padding with 0's is done in grid formation deficiency.

Step 9: File has been encrypted by DSA algorithm.

Step 10: Reverse process has been proceed to get original file

Encryption

Broadly our technique can be divided into 3 phases

1) Grid transposition of data.
2) Columnar transposition based on session key.
3) RSA encryption of key.

VI. RSA ENCRYPTION OF KEY

The key generated is encrypted based on the public key given to the sender. Instead of encrypting the entire key at a time, it is first divided into N/2 decimal parts where N is grid size. Now each part is considered and is encrypted by using the RSA algorithm. Each part produces 4 bytes of data. Hence a 32 sized grid has an encrypted key written to the file of size 512. Similarly for 64-sized grid it is 1024 and

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

so on. This process of encrypting the key is called encapsulation. **RSA** is one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977.

RSA algorithm

1. Assume any two prime numbers P, Q
2. Calculate N = P * Q
3. Calculate Z= Φ (N) = Φ (P * Q) = Φ (P) * Φ (Q) (According to modular arithmetic) = (P-1) * (Q-1)
4. Assume a value 'e' i.e. relatively prime to Z and e < Z and gcd (e , Z) = 1
5. Calculate d, such that e * d ≅ 1 (mod Z) ≅ 1 (mod Φ (N))
6. Cipher (C) = (m ^ e) mod N Plaintext (m) = (C ^d) mod N

Thus our key generated is both complex and secure.

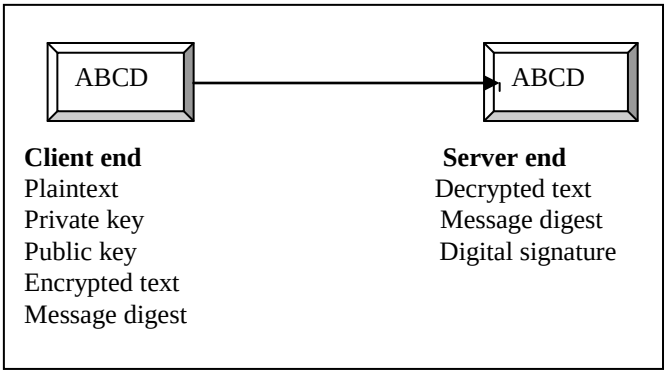
VII. DECRYPTION

For decryption the reverse process is applied. in decryption. It is the process of extracting the original information (plain text) from the encrypted data (cipher text). The word decryption refers to the reverse process to make the encrypted information readable again. The individual bytes from the file are combined and the combined result is decrypted using the private key at receiver's side. Hence the session key is obtained. The reverse process is done i.e. columnar re-transposition and anti grid transposition to get the plain data.

Example: Lets message is ABC

ASSCI of A is=65(01000001) it will divide from 13 and 5 than we will add 2 and new value is(65+2)=67.So we will replace A with C. ASSCI of B is=66(01000010) it will divide from (2,3,6,11,22,33) than we will add 5 and new value is(66+5)= 7.So we will replace B with G. And so on…….

So original file will change.



Process of Security through Encryption

VIII. FUTURE SCOPE

- This research will be useful where high security needed.
- It takes less time to execute and provide high scalable security
- DSA algorithm is very useful, that we have used in our paper that will help others understanding the complete project. So that makes it easy to reuse
- Today encryption is a challenge for everyone; our project gives a new approach to everyone.
- It can protect communication and stored information from unauthorized access and disclosure
- The first one is to ensure message integrity (check if the message has been tampered with) and the second one is to ensure non-repudiation (ensure that the sender of the message cannot refuse having sent it). Using a message digest as the base, how can we achieve this? Well, we cannot. And this is where a digital signature steps in. A digital signature can be used to guarantee, beyond doubt, the validity of message integrity and that of non-repudiation. Let us understand this now. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. For this purpose, let us quickly review the message digest computation process.
- It can be further used in VANET kind of a scalable environment.
- Application can easily be used at client server architectures

IX. SECURITY ATTACKS ON CRYPTOGRAPHY

Attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. A system must be able to limit damage and recover rapidly when attacks occur. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. Security attacks can happen at the application level or the network level. A system must be able to limit There are two types of attacker which attack during the encrypted and decrypted the message.

a. Passive attack
b. Active attack
c. Distributed attack
d. Insider attack
e. Close-in attack

Passive Attack

A passive attack are those attack which attack on a communication system and attack only read messages but he does not alter the messages. It includes traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing information such as passwords. Passive attack results in the disclosure of information or data files to an attacker without the content and knowledge of the user

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

Active Attack

In an **active attack,** the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

Distributed Attack

It provides the security to the whole computer. Attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses.

Insider Attack

Internet attack is the attacking attempts to intercept read or alter information moving between two computers. Attacks are associated as well as with wired communication systems. Attacks on a system or network where the intruder is someone who authorized access to the network. An internal intrusion detection system is on measure that can help organizations limit the risk from insider attack

Close-in Attack

Close-in attack is those attack which physically close to the network components, data and system. Close in attacks consisting of regular individual attaining close physical proximity to the networks. The most popular example of close-in attack is social engineering. The attacker compromises the network with a person through an e-mail message or phone call.

Principle challenges in Distributed Environment are

- Data integrity- ensuring that data is not modified during transmission
- Data privacy- ensuring that data is not disclosed during transmission
- Authentication- having confidence that users hosts and clients identities are correctly known
- Authorization- giving permission to a user, program ,or process to access an object or set of objects

It establishes user identity is also primary concern in distributed environments little confidence in limiting privilege by user. For example, unless you have confidence in user authentication mechanism, how can you be sure that user connecting to a server A from client B really is user? Furthermore, you need to have confidence in the way clients and servers are made to known to one another over the network so that you have assurance. Security is an important thing for all kinds of networks. . It enables you to store information and transmit it across insecure network so that it cannot be read anyone except recipient. In order to rescue our data from intruders we need CRYPTOGRAPHIC techniques. Cryptography is the science of using mathematics to encrypt and decrypt the data. Encryption is the process to convert the message from plain text to cipher text and the decryption is the reverse process which is used to convert the message from cipher text.

X. CONCLUSION

As we know that internet and information sharing has a positive and negative impact. One of the negative impacts was the large increase in new information threats. These computers incidents have raised a number of concerns about how information is secured and maintained. Security is often view as the need to protect the information and network operation. So we apply security in encryption through grid technology The project ‘plays a vital role in our career. We worked on various modules of project and learnt that in any encryption project requirements are not static but keep on growing and even changing. The ever growing requirements can be ceased. This project has been quite interesting for us. The specialty of the Project is that it reduces the time. We have worked up to our best level to make this project a user friendly one. So that the users are able to use this project freely and with no difficulty for that several instructions and encryption are also applied at different levels.

REFERENCES

[1] Z. Lu, X. Lu, W. Wang, and C. Wang. Review and evaluation of security threats on the communication networks in the smart grid. Military Communications Conference2010, 2010.

[2] P. McDaniel, S. McLaughlin, "Security and Privacy Challenges in the Smart Grid,” IEEE. Security & Privacy, vol.7, pp.75-77, May-June, 2009.

[3] Fengjun Li, Bo Luo, Peng Liu, "Secure information Aggregation for Smart Grids Using Homomorphic Encryption, " in Proc.2010 First IEEE International Conference on Smart Grid Communications, pp. 327-332.

[4] J. Coron, "What is cryptography?" IEEE Security and Privacy, vol.4, pp. 70-73, 2006.

[5] Davis, J., "Information Systems Security Engineering: A critical Components of the Systems Engineering Lifecycle", ACM SIGAda, 2004, pp.13-17. (Pubitemid 40730715)

[6] Simmonds, A; Sandilands, P; van Ekert, L (2004) Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285, pp.317–323.

[7] Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.

[8] Sanchez-Avila, C. Sanchez-Reillol, R, ―The Rijndael block cipher (AES proposal): A comparison with DES‖, 35th International Conference on Security Technology 2001, IEEE.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

[9] Punita Mellu & Sitender Mali, ―AES: Asymmetric key cryptographic System‖, International Journal of Information Technology and Knowledge Management, 2011, Vol, No. 4 pp. 113-117.

[10] Mohamed A.Haleem, Chetan N.Mathur R.Chandramouli,K.P.Subbalakshmi,"OpportunisticEncryption: A tradeoff between Security and Throughput in Wireless Network" IEEE Transactions on Dependable and secure computing, vol. 4,T.Muthumanickam,"PERFORMANCE ANALYSIS OF CRYPTOGRAPHIC VLSI DATA", IRACST –International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol. 2, No. 1, 2012.

[11] V. Dehalwar, R. K. Baghel, M. Kolhe. Multi-Agent based Public Key Infrastructure for Smart Grid, The 7th International Conference on Computer Science & Education (ICCSE 2012) July, 2012. Melbourne, Australia.

[12] Y. Liu, P. Ning, and M. Reiter. False data injection attacks against state estimation in electric power grids. ACM CCS, 2009.

[13] L. Xie, Y. Mo, and B. Sinopoli. False data injection attacks in electricity markets. IEEE Smart Grid Comm, pages T. Baumeister. Literature review on smart grid cyber security, Technical Report,

[14] A. R. Metke and R. L. Ekl. Security technology for smart grid networks. IEEE

[15] Punita Mellu & Sitender Mali, ―AES: Asymmetric key cryptographic System‖, International Journal of Information Technology and Knowledge Management, 2011, Vol, No. 4 pp. 113-117.