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

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

Cryptography and its two Implementation Approaches

Gagandeep shahi[1], Charanjit singh[2]

Research Scholar, Dept. of Computer Science Engineering, RIMT- IET, Mandi Gobindgarh, India[1]
Assistant Professor, Dept. of Computer Science Engineering, RIMT- IET, Mandi Gobindgarh, India[2]

Abstract:In the modern digital world inviolability of the crucial facts is an essential part for data security. The entire world becoming a village due to the digital data conveys through network of networks called internet. With availability of network everywhere the common man perform transactions such as buying and selling the products called e-commerce, cash submission and withdrawal from bank with the help of e-banking etc. Network may be insecure where the people transmitting their decisive data, valuable information in the form of conspicuous passwords etc. Third parties like hackers who do not have the authority can hack the data. They can destroy confidentiality of the facts, integrity of the facts as well as availability ofthe facts. To prevent this, cryptography must be there. In this paper we will discuss about the cryptography and its two implementation approaches Known as Peer to Peer (P2P) Trusted Third Party Cryptography Approaches which is based upon Client Server Computing.

Keywords: Cryptography, Trusted Third Party, Peer to peer (P2P). Same key Cryptography, Different Key Cryptography, and Hash cryptography

I. INTRODUCTION

In the modern winged electronic information barter, every person from each part of the world communicates through cyber space without thinking of a moment about security of the information that we conveyed. So middlemen, who do not have authority can hack the crucial information through the cyberspace. Cryptography is a technique of hiding the plain information from the web thugs. By using cryptography we can assist this shaky information by secrete writing on our computer network. There are two basic approaches to implement cryptography on the computer networks called Trusted Third party or centralized approach and Peer to Peer cryptography approach. As the name suggest, in Trusted Third Party cryptography approachsecurity of data depends upon the centralized control which may be single server or multiple server. Peer to peer does not have this type of centralized control.

II. CRYPTOGRAPHY ANDITS TYPES

Cryptography is the art and science of hiding important and secret information from being infringed upon by unauthorized persons as in [1]. Cryptography is not only the art and science; it is also a mathematical approach that converts the plain information into the unreadable format, so that only the valid receiver can understand that crucial information. In simple words cryptography is an approach that work like a safeguard of the message that unable the web thugs or middlemen to understand the actual meaning of the message who have no authentication. Cryptography uses the process of transposition and substitution of the characters to hide and retrieve the data. At the sender side we call it Encryptionshown in Fig.1 and at the receiver side we called it decryption shown in Fig.2.We use the various keys to encrypt an decrypt the data. Keys are the special digital functions or methods that convert the plain text into inscribe format and it's vice versa. Every element of the network have two keys namely private or personal key which is known to a particular person and public key which is known by all persons in the network. There are three types of cryptography.

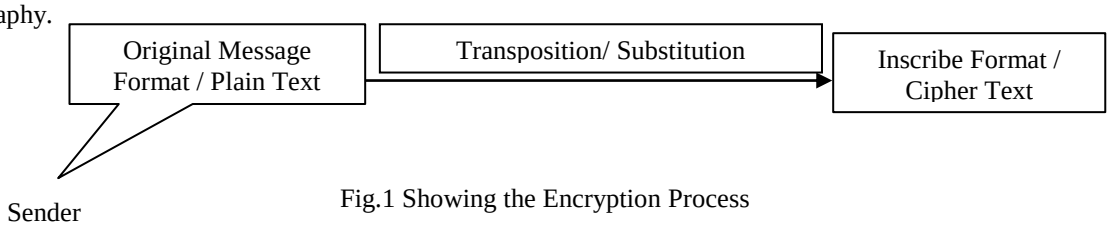

Fig.1 Showing the Encryption Process

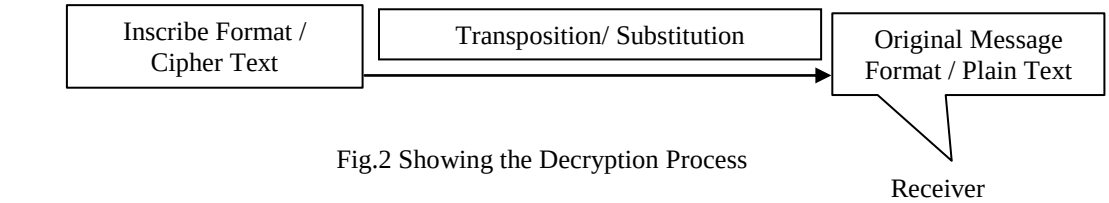

Fig.2 Showing the Decryption Process

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

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

A. Same key cryptography or Private key cryptography

In this type of cryptography the receiver and sender applies the same key to encrypt and decrypt the message or recover the plaintext from cipher text and vice versa, so thistype of cryptography is also known as symmetricencryptionand decryption. Fig.3 is showing the whole process of encryption and decryption which is carried out through receiver's private key. Through this cryptography form, it is obvious that the secretkey must be known to both the sender and the receiver that why it is known as private key cryptography.The biggest difficulty with this approach, of course, is the distribution of the key as in [2].Transmitting the secret key on insecure network can also destroy the security.

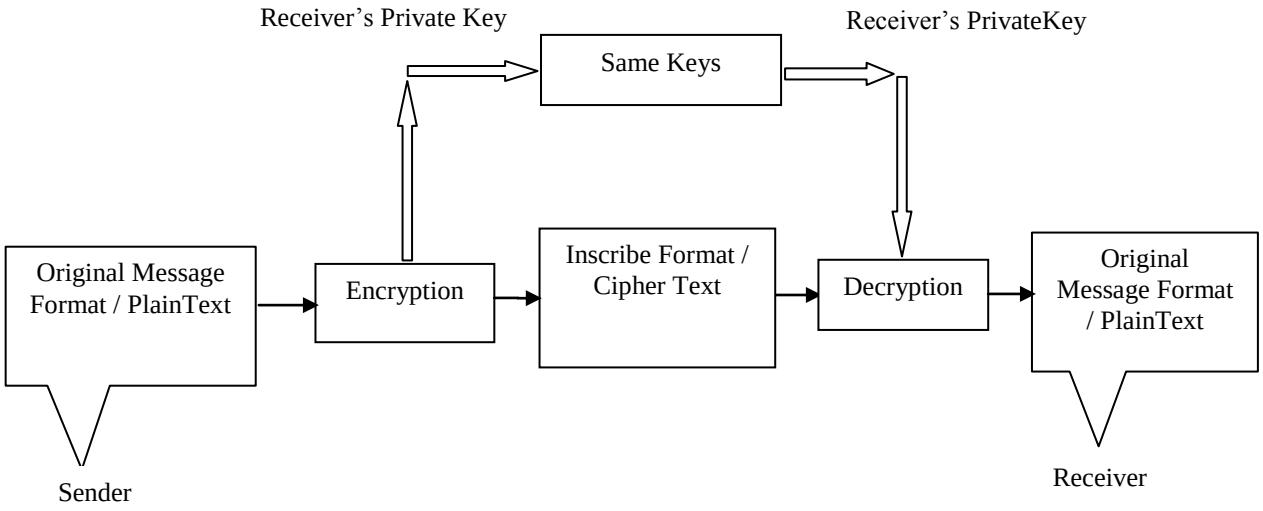

Fig.3 showing the Same key cryptogroaphy

B. Different key cryptography or public key cryptography

In this type of cryptography, the receiver and senderapply the Different keys to encrypt and decrypt the message or recover the plaintext from cipher text and it's vice versa.Thistype of cryptography is also known as asymmetricencryptionand decryption.Fig.4is showing the whole process where receiver's public key is used for encryption and receiver's private key is used for decryption.In public key cryptography, each user or the workstation take part in the communication have a pair of keys, a public key and a private key and a set of operations associated with thekeys to do the cryptographic operations. Only a particular user/device knows the privatekey whereas the public key is distributed to all users/devices taking part in thecommunication. Since the knowledge of public key does not compromise the security of thealgorithms, it can be easily exchanged online as in [3].

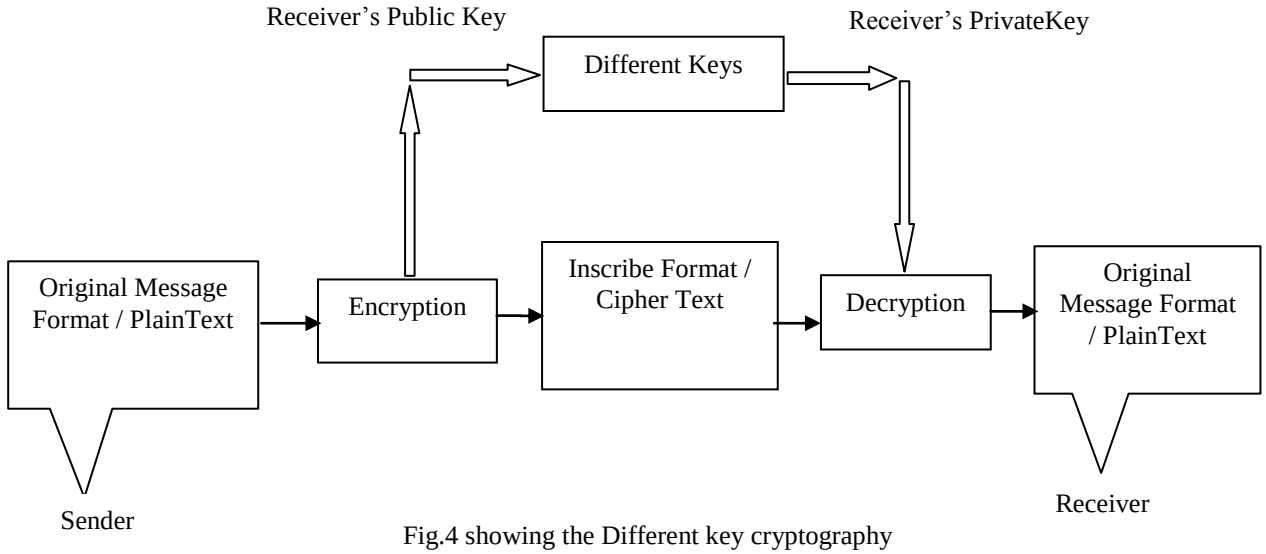

Fig.4 showing the Different key cryptography

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

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

C. Hash cryptography

Hash cryptography does not need any type of key to encrypt and decrypt the message. Private Key or public key cryptography does not take guaranty of the original message received by receiver. There may be a possibility of message tempering during the way by intruders. To stop this message tempering, sender uses the hash function on the original message and create the message hash. After this sender attach the message hash with original message and send to receiver. At the receiver's side,receiver again performs the similar hash function on the message that was performed by the sender side and again creates the new message hash. At last new message hash matches with attached message hash.Ifboth message hashes match, there were no tempering in the message and accept it. Otherwise message was tempered during the way and must be rejected.Hash cryptography uses algorithms to facilitate communicationand the hash key normally provides a digital fingerprint, making sure that the file is not corrupted or infected with virus as in [1].

III. IMPLEMENTATION APPROACHES OF CRYPTOGRAPHY

An implementation approach of cryptography defines the way of implementing the cryptography on the computer networkto secure the transmission over the network. There are two implementation approaches:

A. Trusted Third Party Cryptographyor Trusted Centre CryptographyApproach

In trusted party approach as name suggest an administrator hire the third party (government, distributor, organisation etc.) for the security of the network who is always responsible for the encryption\decryption, validity and authenticity of the data, so that sender and receiver of the data can freely send or receive it without thinking for a moment about the network security. All the communication between workstations of the network always goes throughthe trusted third party.Trusted third party may have single or more servers for validity, authentication and the encryption/decryption etc. of the data. Fig.5 is depicting the Trusted Party with its two servers named as verification and certification servers. Network security starts with authenticating the user, commonly with a username and a password. Since this requires just one detail authenticating the user name —i.e. the password, which is something the user 'knows'— this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g. a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g. a fingerprint or retinal scan)as in [4]. Trusted centre take care of all these factors using digital signatures for verifying the message coming from the valid user and validate it through thedigital certificate.The idea of a "digital signature" first appeared in Diffie and Hellman's seminal paper, New Directions in Cryptography [DH76]. They propose that each user A publish a "public key" (used for validating signatures), while keeping secret a "secret key" (used for producing signatures) as in [5].A certificate consists of a public key, an identifier of the key owner, and the whole block signed by a trusted thirdparty.This approach purely based upon client/server computing as in [6].Client/server computing has gained popularity in the recentyears due to the proliferation oflow-cost hardware and the increasinglyapparent truth of the theory that amodel relying on monolithic applicationsfails when the number of usersaccessing a system grows too high orwhen too many features are integratedinto a single system as in [7].

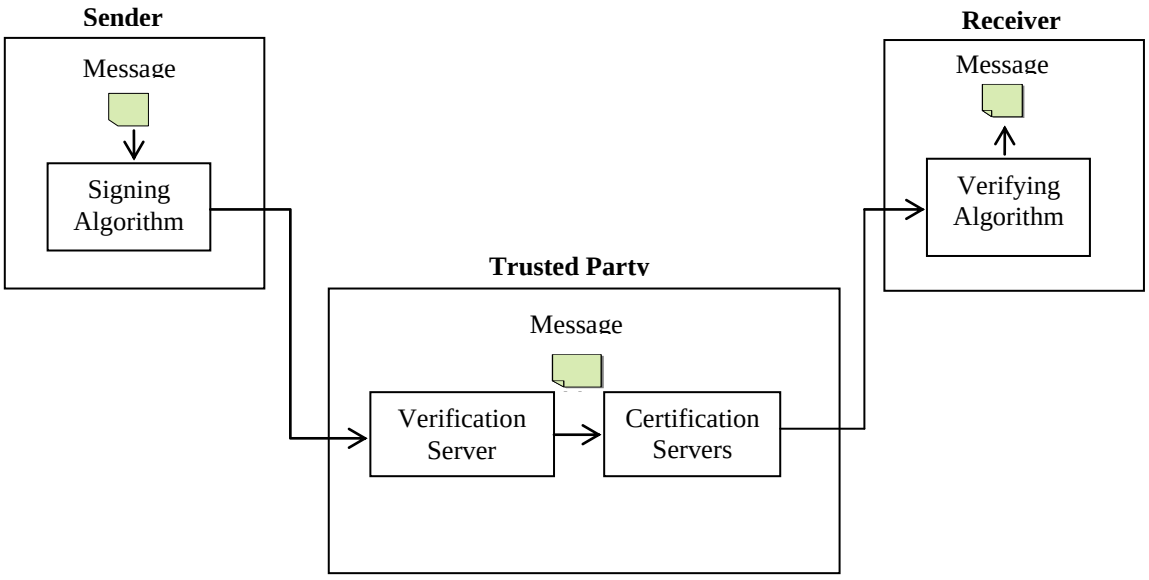

Fig.5 showing the communication between Sender and Receiver through the trusted party

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

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

B. Peer to peer cryptography approach

This approach is based upon the peer to peer computing.The term "peer-to-peer" refers to a class of systems and applications that employ distributed resources to perform function in a decentralized manner. The resourcesencompass computing power, data (storage andcontent), network bandwidth, and presence (computers,human, and other resources) as in [8]. In this approach, workstations never use any trusted party for the security of data.They rely on the cryptography algorithms.This approach work in two sessions, in the first session workstations exchanges their keys and in the second session, we send or receive the encrypted messages. Encryption/decryption is always performed by the application builds from any cryptography algorithm. Peer to Peer secure communication between two workstations of the network is shown in Fig.6..

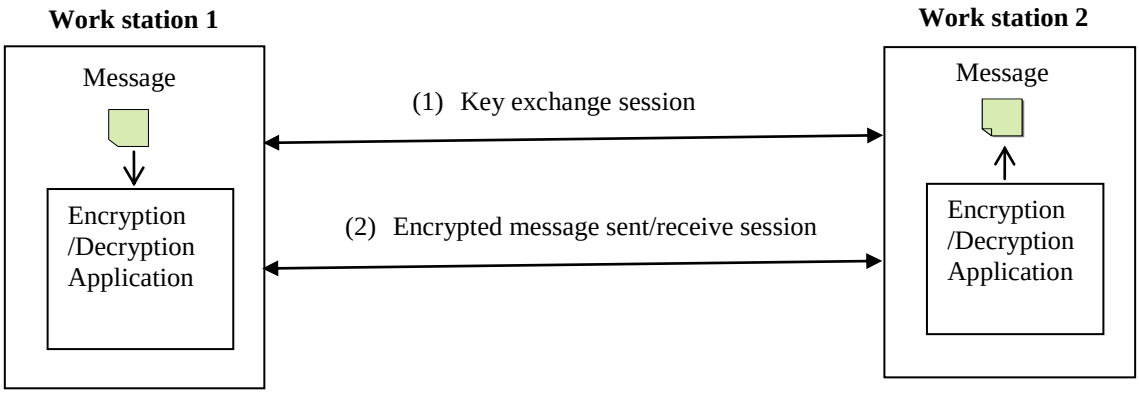

Fig.6 Peer to Peer(P2P) Cryptography between two workstations of the network

In Section 'A' and Section 'B' we discussed the two implementation approaches of cryptography. Some differences between both approaches are shown in the TABLE 1.

TABLE I
DIFFERENCE BETWEEN TWO IMPLEMENTATION APPROACHES OF CRYPTOGRAPHY

Serial Number	Parameters	Trusted Third Party CryptographyApproach(TTPCA)	Peer to Peer Cryptography Approach(P2PCA)
1	Type of computing	It's based upon client server computing.	It's based upon distributed computing.
2	Encryption/Decryption	In TTPCA, Encryption/Decryption depends upon the servers of the trusted party.	P2PCA never relies on centre servers so its encryption/decryption depends upon the cryptography algorithms.
3	Cost	Cost of security can be high because we have to hire any trusted party.	P2PCA uses internal network resources which costs low compare to TTPCA.
4	Security	We hire the external party for security of the data so there may be better security because integration, validation, authentication etc. depend upon the trusted party servers and If trusted centre hacked by the intruder then all security can be destroyed.	In P2PCA message security depends upon the strength of techniques which we had used for encryption and decryption. If algorithm used for security fulfill the security issues like integrity, validity, and authentication etc. then onlyit can provide better security. Normally TTPCA always have the better security.
5	Burden	In the TTPCA, burden of the security of the data is totally shifted upon the third party. Sender and Receiver get assurance of security with security certificates provided by the trusted third party.	In P2PCA, Security of the data is always aresponsibility of the network administrator. he install the cryptography applications on the workstations. Once right application installed there is no burden of security. Sender and receiver can enjoy instant messaging.

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

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

IV. CONCLUSION

Data security is a hot issue in this modern digital era. Cryptography fulfills the security issues like integrity of data, confidentiality of data, availability of data and verification/validation of the data. We have already discussed the various techniques of the cryptography with its two implementation approaches named as TrustedThird Party Cryptography Implementation Approach(TTPCA) Peer to Peer Cryptography Approach(P2PCA).According to the situation we can use these approaches with the help of available resources in our network.

ACKNOWLEDGMENT

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 Mr.Charnjit Singh for his great efforts of supervising and leading me to accomplish this fine work.

REFERENCES

1. Dr. Qais Faryadi (2013), "Does Data Security Matter? The Case for Cryptography", the 2nd International Conference on Computer Science & Computational Mathematics (ICCSCM), 2013.
2. Ayushi(2013), "A Symmetric Key CryptographicAlgorithm', International Journal of Computer Applications", Vol. 1-NO.15, pp. 0975 – 8887, 2013.
3. Anoop(2005), "Public KeyCryptography-Applications Algorithms and Mathematical Explanations", anoopms@tataelxsi.co.in,2005.
4. Sumedha Kaushik,**Ankur**Singhal,"Network Security Using Cryptographic Techniques", Volume 2, Issue 12,pp. 105-107, 2012.
5. ShafiGoldwassar, SilvioMicali and Ronald L. Rivest, "A Digital Signature Schemes Secure AgainstAdaptive Chosen-MessageAttacks",Society for Industrial and Applied Mathematics,Vol. 17, No. 2, 1988.
6. William Stallings, "Cryptography and Network SecurityPrincipal and Practice", Pearson Education, Inc., publishing as Prentice Hal, 2011.
7. Scott M. Lewandowski, "Frameworks for Component-Based Client/Server Computing", ACM Computing Surveys", Vol. 30, No. 1, 1998.
8. Ernesto Damiani,De Capitani di Vimercatiand StefanoParaboschi, "A ReputationBased Approach for Choosing ReliableResources in PeertoPeer",Proceedings of the 9th ACM conference on Computer and communications security,ISBN: 1-58113-612-9, 2002.
9. Pankaj R. Patil and D.R.Patil,"Distributed private key for P2P network message security", World Journal of Science and Technology, Vol. 2(3), pp. 122-126, 2012.
10. Tobin White, "Encrypted objects and decryption processes: problem-solving with functions in a learning environment based on cryptography", Vol.72, issue.1, pp. 17-37,2009.
11. Gunjan Gupta,Rama Chawla(2012), "Review on Encryption Ciphers of Cryptography in Network Security", Proceedings of the International Conference on Data Engineering",Volume 2, Issue 7, ISSN: 2277 128X, 2012.

BIOGRAPHY

Er. Gagandeep Shahi is a research scholar Pursuing Master of technology in Computer Science Engineering from RIMT- IET College Mandi Gobindgarh, Punjab (India). He received the degree of Bachelor of Technology in Computer Science Engineering from Ludhiana College of Engineering & Technology Katani Kalan Ludhiana, Punjab (India).He is also a Diploma holder in Computer Science Engineering from Guru Nanak Dev Polytechnic College Ludhiana , Punjab(India) he is havingalmost one and half yearteaching experience. His area of interest is Network security issues faced by the users in the computer networks and RDMS.

Er. Charanjit Singh is highly qualified teacher with a rich experience of 9.5 years in Teaching & Administration in Educational Institutes.He is presently serving as Assistant Professor in Computer Science Department of RIMT-IET, Mandi Gobindgarh. Er. Charanjit Singh completed his M.Tech. in Computer Science & Engineering from Guru Nanak Dev college of Engineering & Technology, Ludhiana. His area of interest includes Distributed systems, computer networks, computer architecture and digital hardware design. He is pursuing his Ph.D. in Computer Science and Engineering.

.