



Mechanism to Secure Intra Organization Communication Between users' which are Isolated from Internet

Isha Kharbanda*
NIEIT, New Delhi,
India

Karamjit Singh
K.R.M.D.A.V. College, Nakodar,
India

Abstract: *In an organization communications between various departments or between various employs are in plain text means transition the words, letters, or files to other recipient are in readable form. By sniffing the traffic, any non legitimate employ can easily read the files which are secret from any other unauthorized employs and departments of the organization. This will cause problem regarding of confidentiality, integrity and authenticity. In organization, major problem during communication is how to achieve Confidentiality, integrity as well as authentication. The objective of the paper is to secure the intra organization communication by achieving these basic components of security over information.*

Keywords: *Cryptography, secure communication, Encryption, Decryption, public-key infrastructure.*

I. Introduction

A Public key Infrastructure is generally considered to be associated with three primary services:

- Authentication is the assurance to one entity that another entity is who he, she, or it claims to be.
- Integrity is the assurance to an entity that data has not been altered (intentionally or unintentionally) between "there" and "here" or between "then" and "now."
- Confidentiality is the assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended.

Authentication

Authentication, the assurance that an entity is who he, she, or it claims to be, typically finds application in two primary contexts, entity identification and data origin identification.

Integrity

Data integrity is the assurance of no alteration: The data (either in transit or in storage) has not been undetectably altered. Clearly, such assurance is essential in any kind of business or electronic commerce environment, but it is desirable in many other environments as well. A level of data integrity can be achieved by mechanisms such as parity bits and Cyclic Redundancy Codes (CRCs). Such techniques, however, are designed only to detect some proportion of accidental bit errors; they are powerless to thwart deliberate data manipulation by determined adversaries whose goals are to modify the content of the data for their own gain.

To protect data against this sort of attack, cryptographic techniques are required. Thus, appropriate algorithms and keys must be employed and commonly understood between the entity wanting to provide data integrity and the entity wanting to be assured of data integrity. The PKI service of integrity can be extremely useful in meeting the needs of both entities because it is the framework through which algorithm selection and key agreement can take place. Furthermore, such negotiations can occur in a way that is completely transparent to the entities involved so that integrity can be assumed in all PKI-related data transactions. (This situation changes only when integrity verification fails for some specific piece of data, in which case the user must be notified so that appropriate action can be taken.)

Confidentiality

Confidentiality is the assurance of data privacy: No one may read the data except for the specific entity (or entities) intended. Confidentiality is a requirement when data is:

- Stored on a medium (such as a computer hard drive) that can be read by an unauthorized individual
- Backed up onto a device (such as a tape) that can fall into the hands of an unauthorized individual Transmitted over unprotected networks.

Algorithms

A number of public-key algorithms exist, and each is suitable for one or more of the services:

RSA

The algorithm proposed by Ron Rivest, Adi Shamir, and Len Adleman in 1978 known as RSA, is one of the earliest and most versatile of the public-key algorithms. It is suitable for encryption/decryption, for signing/verification (and, therefore, for data integrity), and for key establishment (specifically key transfer). It can be used as the basis for a secure pseudorandom number generator as well as for the security in some electronic games. Its security is based on the

difficulty of factoring very large integers. The current state of factoring research suggests that RSA keys should be at least 1,024 bits long to provide adequate security for the next several years or more.

DSA

The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard (FIPS) publication of NIST of the U.S. Department of Commerce. It is a variant of the ElGamal signature mechanism. The DSA was designed exclusively for signing/verification and therefore also for data integrity. Other algorithms in the ElGamal family can be used for encryption/decryption and therefore key transfer, if what is being encrypted and decrypted is a symmetric key. The security of these algorithms is based on the difficulty of computing logarithms in a finite field. The current state of research with respect to discrete logarithms suggests that DSA keys should be at least 1,024 bits long to provide adequate security for the next several years or more.

DH

The algorithm that Diffie and Hellman proposed, known as DH, is a wonderful example of elegance and simplicity. The earliest public-key algorithm, it is exclusively a key establishment, specifically key agreement, protocol. Each of two entities uses its own private key and the other entity's public key to create a symmetric key that no third entity can compute. The algorithm derives its security from the difficulty of computing logarithms in a finite field. As with DSA, the current state of research with respect to discrete logarithms suggests that DH keys should be at least 1,024 bits long to provide adequate security for the next several years or more.

SHA-1

The Secure Hash Algorithm SHA-1, a slight revision of the original Secure Hash Algorithm SHA, is described in a NIST FIPS publication. This hash algorithm was designed specifically for use with the DSA but can be used with RSA or other public-key signature algorithms as well. Its design principles are similar to those used in the MD2, MD4, and especially MD5 hash functions proposed by Ron Rivest. Current computational capability suggests that the size of the SHA-1 hash value, 160 bits, provides adequate security for at least the next several years. Hash functions are not public-key algorithms but are included here because digital signature algorithms are always used in conjunction with hash algorithms to provide the services of signing/verification and data integrity. Thus, they are an essential component of the digital signature and integrity security services.

II. Objective

The objective of the paper is to secure the intra organization communication by achieving confidentiality, integrity as well as authentication over information.

In organization, employs/departments able to securely communicate i.e. sending files, documents etc. with each other in secure manner. As concern with performance, maintains, cost and reliability it is more effective and easy to use in intra organization communication.

III. Mechanism for Secure Communication

Secure intra organization communication enable communication within organization in secure manner. In organization, employs/departments able to securely communicate i.e. sending files, documents etc. with each other in secure manner. In this paper use of, PKI (public-key infrastructure) enables the secure exchange of data over unsecured media. PKI is the underlying cryptographic security mechanism for digital certificates and certificate directories, which are used to authenticate a message sender. PKI is the standard for authenticating commercial electronic transactions, Understanding PKI. Asymmetric ciphers make use of two related but different keys. In this key pair, the keys are sufficiently different that knowing one does not allow derivation or computation of the other, even for determined adversaries with a lot of computing power at their disposal. This means that one of the keys may be made publicly available. The idea that one of the keys in this pair can be revealed publicly was so radical and appealing that this whole method of protecting data quickly became known as public-key cryptography.

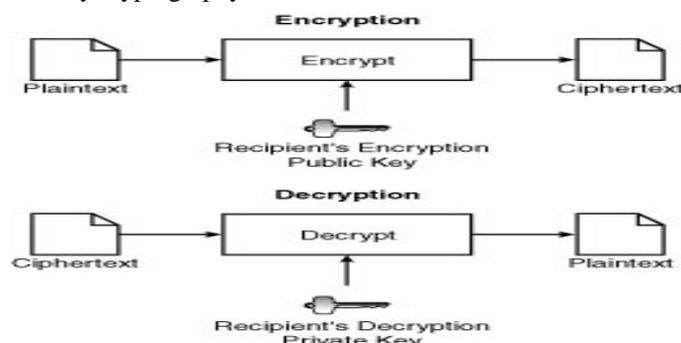


Fig. Error! No text of specified style in document.: Public-Key Cryptography

Plain text is first encrypted with public key of recipient to make cipher text, after that recipient can decrypt it with her/his private key. Public key is accessible to all the users but private key is not accessible to other, If any users compromise her/his private key then we will consider security is not too more on compromising private key.

In Secure communication, there will be use of two things one is crypto pad that will generate public/private key pairs and for sending encrypted data, will use file sharing web server.

Process:

Key pair generation and public key store on file sharing web server:

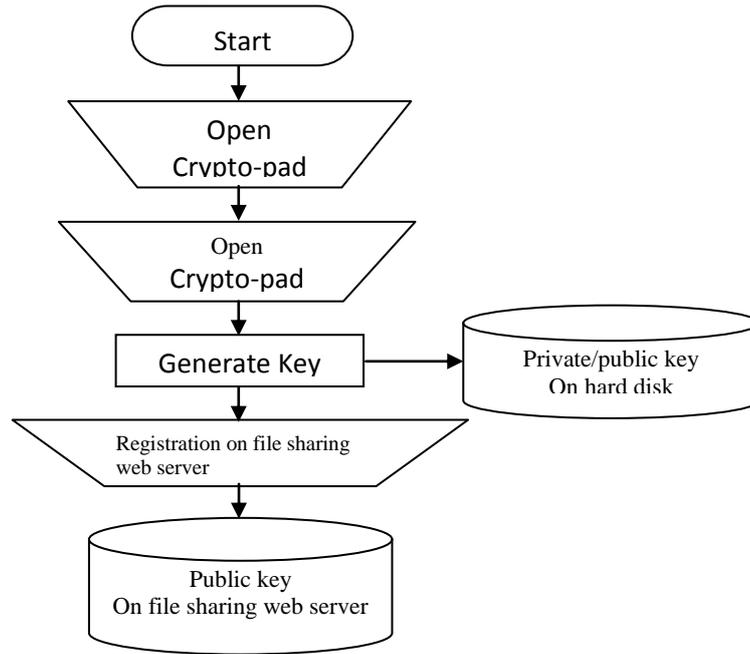


Fig. 2: Key pair generation and public key storage

Firstly, users will open crypto-pad and generate key pair i.e. public key and private key after generation of key pair users will store public and private keys on hard disk of own computer.

After generation of key pair users will register on easy file sharing web server. And after registration, users will login into file sharing web server and upload public key on own folder that will be accessible for all the users. From that folder other users will get public key for encryption process to send encrypted message to recipient. In this process user will be able to receive encrypted data from others.

Encryption process at sender side:

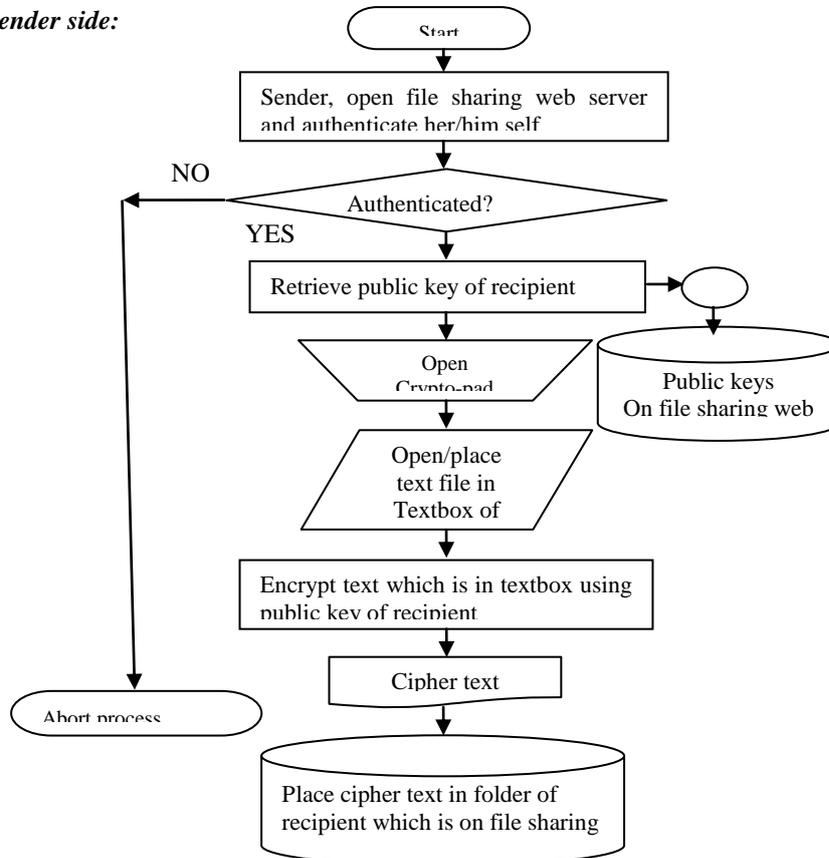


Fig. 3: Encryption Process

During Encryption process, sender who wants to send message to recipient, firstly user will login onto file sharing web server and authenticate him/herself. If user is authenticated then he/she will retrieve public key of recipient from the recipient folder and after that user will open crypto-pad and will open file/message with the use of browse option that is on the crypto-pad. When user open file on crypto-pad he/she will open the recipient public key and encrypt that message. Place that encrypted message at recipient folder to whom user want to send message.

Decryption process at receiver side:

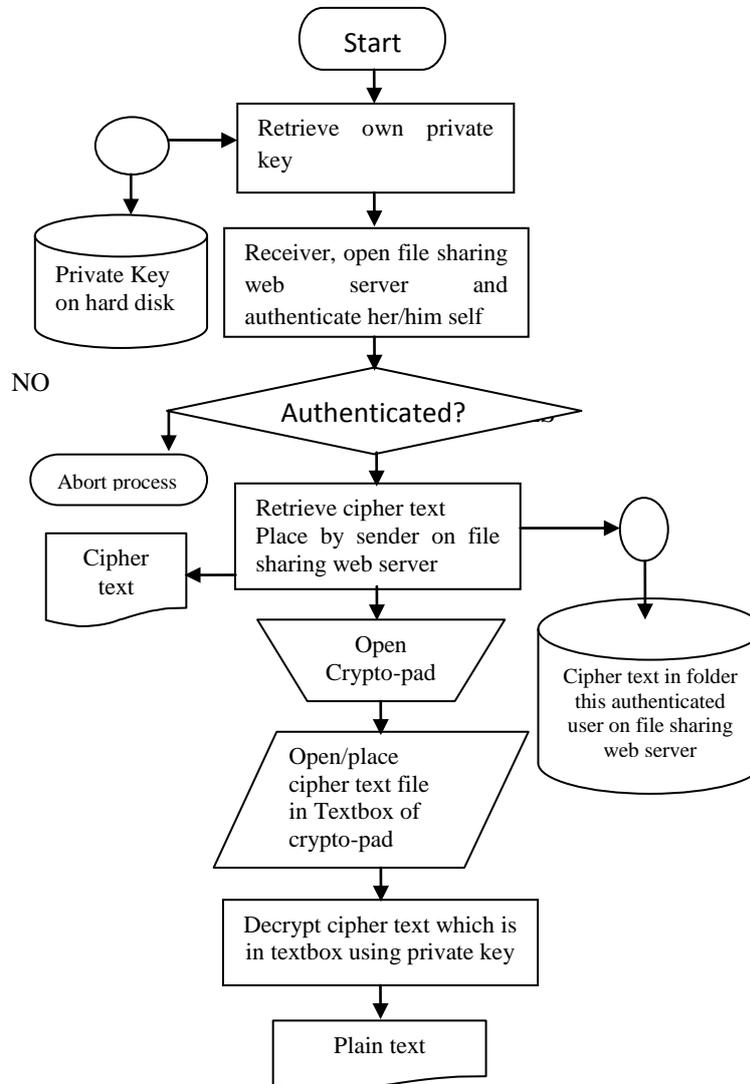


Fig. 4: Decryption Process

In decryption process, first receiver will retrieve the private key to decrypt the message from hard drive, which was stored on hard drive during key pair generation. After that receiver will open the browser and will authenticate her/himself over file sharing web server to retrieve received message and place message on hard drive after that receiver will open crypto-pad and open message in crypto-pad then click on decryption button to decrypt message. By this, receiver will decrypt message and receiver will retrieve the message from sender with full of confidentiality.

IV. Conclusion

Secure intra organization communication enable users to communicate with each other by full of confidentiality. Unauthorized user will not able to see communication between two users. Each department of organization can communicate with other department or within department with full of confidentiality. Let's suppose accounts department wants to transfer account related data to head of organization then by the use of this proposed technique they will be make secure communication and transfer data to head of organization in secure manner.

References

[1] Karamjit Singh, Isha Kharbanda and Navdeep Kaur. "Security issues occure in Cloud computing and their solutions", International Journal on Computer Science and Engineering (IJCSSE), Vol 4, Issue 5, pp. 945-949 May.2012.

- [2] Carlisle Adams, Steve Lloyd “*Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition*”.
- [3] Sahai and B. Waters, “Fuzzy identity-based encryption,” *Advances in Cryptology-EUROCRYPT 2005*, pp. 457–473, 2005.
- [4] Liazhu Dai and QinZhou, “*A PKI-based Mechanism for Secure and Efficient Access to Outsourced Data*”, 2010 International Conference on Networking and Digital Society 640-643
- [5] William Stallings: “*Cryptography and Network Security*” [book style].
- [6] Karamjit Singh, Isha Kharbanda. “*Role of public key infrastructure in Cloud Computing*”, IJAIR, 340-342, ISSN 2278-7844.
- [7] liazhu Dai and QinZhou, “*A PKI-based Mechanism for Secure and Efficient Access to Outsourced Data*”, 2010 International Conference on Networking and Digital Society 640-643