Network Security and Cryptography: A Comprehensive Approach to Protection

Robert T. Johnson[1], Linda M. Davis[2]
[1]Department of Electrical Engineering, University of Toronto, Ontario, Canada
[2]Department of Computer Engineering, University of British Columbia, Vancouver, Canada

ABSTRACT

With the advent of the World Wide Web and the emergence of e -commerce applications and social networks, organizations across the world generate a large amount of data daily. Data security is the utmost critical issue in ensuring safe transmission of information through the internet. Also network security issues are now becoming important as society is moving towards digital information age. As more and more users connect to the internet it attracts a lot of cyber-criminals. It comprises authorization of access to information in a network, controlled by the network administrator. The task of network security not only requires ensuring the security of end systems but of the entire network. In this paper, an attempt has been made to review the various Network Security and Cryptographic concepts.

Keywords: network security, cryptography, decryption, encryption.

I. INTRODUCTION

Network security is the protection of the access to the files and data as well as misuse from the unauthorized users, hackers. Network security deals with the problems of authentic messages being taken and replayed. It is the effort to create a secure computing platform. The action in question can be reduced to operations of access, modification and deletion. Network security used in public sector as well as private sector. Usually it is used in day to day jobs; like doing transactions and communications among businesses, government agencies or individuals. Networks security can be used private, like within a company, and others that might be open to public access. It is also used in organizations, enterprises, and other types of institutions.

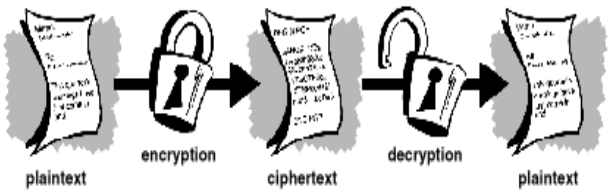
Network Security should include proactive defensive methods and mechanisms to take care of data, network and network devices from external and internal risk as well as danger.

Network security have problems which are divided into four twist around areas: **secrecy, authenticity, non repudiation,** and **integrity control.**

- Secrecy is also called as Confidentiality which means keeping information runaway from unauthorized users.
- Authentication manages whom you're talking to before disclosing sensitive data.
- Non repudiation deals with signatures. It protect either sender or receiver from refuse transmitted message
- Integrity can utilize to a flow message, single message or selected field in message.

All these problems can be managed by using cryptography, which means methods of converting data into unreadable form, at the source only authorized user can access data at the Destination.
Cryptography is a process of converting in a particular form so that only those for whom it is planned can read and action on it.

Cryptography is the methods of using mathematics to encrypt and decrypt data.



Cryptography process

II. CRYPTOGRAPHY

Cryptography is combined with the method of transferring ordinary plain text into not understandable text and vice-versa

Cryptography Process:

- **Clear text**: It is the ordinary text where the messages to be encrypted form known as plain text or clear text.
- **Encryption**: The process of conversion of plaintext into unreadable format for unauthorized users is called Encryption.
- **Cipher text**: Encrypted message is not readable by invalid users is called cipher text.
- **Decryption**: The process of covering the plain text from the cipher text is called decryption.

Encryption and decryption usually can be done with the help of a **key**, i.e. the messages to be encrypted with the help of key. The art of breaking ciphers is called **cryptanalysis**.

The art of arranging ciphers (**cryptography**) and breaking them (**cryptanalysis**) is as a whole known as **cryptology**.

➢ *Fundamental Requirements:*

- **Confidential:** Confidentiality is the secret term. It is fundamental security service of the cryptography. It is the method of keeping data private and Secret so that only the intended recipient is able to understand the data. It is protected from unauthorized users. It is may be called as privacy or secrecy.
- **Authentication:** It is the process of providing proof of identity of the sender to the recipient, so that the recipient can be assured that the person sending the information. Authentication provides the identification of the sender.

Authentication service has two variants −

- **Message authentication** identifies the originator of the message without system that has sent the message.
- **Entity authentication** is assurance that data has been received from a specific entity, say a particular website.

- **Integrity:** Is the method to ensure that information is not modified during its transit or its storage on the network. Any unauthorized person should not be able to modify the information or change the Information during transit.
- It is deals with identifying any alteration to the data.
- **Non-repudiation:** Is the method to ensure that data cannot be cancel. Once the non-repudiation process take place, the sender cannot decline being the creator of the data.

➢ *Security Attacks:*

- **Interruption**: In an attack where obstruction is take place between the transition of one or more of the systems. This leads to systems being unavailable for use that is wastage of system.

- **Interception:** sender send data and unauthorized intercepts the message content and changes it or uses it for malicious purposes. After attack, the message does not remain confidential.
- **Modification**: As the name suggest sender send a message which is modified by unauthorized user Due to this receiver cannot receive the original message sent by sender. Due to this attack affects the integrity of the message.

For above reason user should keep the data secretly during communication. User use Cryptography for processing of data securely without any interruption.

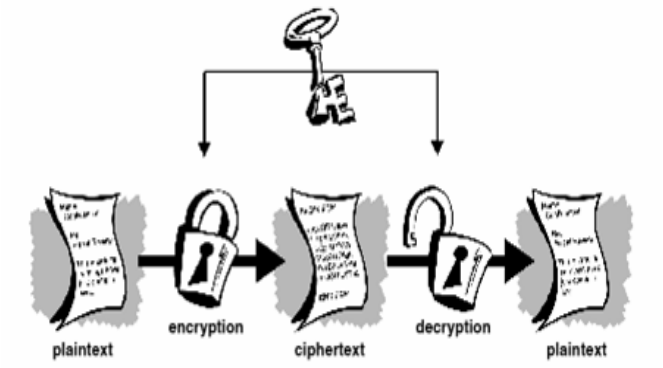
- *Key Process Techniques:*

- **Basic Process:**

M is the original message
K enc is encryption key
M' is the scrambled message
K dec is decryption key
It is "hard" to get M just by knowing M'
E and D are related such that
E(K enc , M) = M'
D(K dec , M') = M
D(K dec , E(K enc , M)) = M
Plaintext—M
Cipher text—M'
Original Plaintext—M
Decryption function—D
Encryption function—E

- **Symmetric-key Encryption: (one key)**

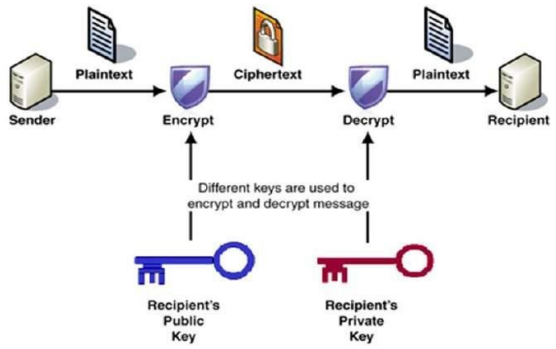
Encryption and decryption are performed by using a same single key. Symmetric-key encryption, also known as shared-key encryption or **secret-key cryptography** (**Private-key method**),. Symmetric-key encryption is an beneficial method for encrypting large amounts of data. Sender and receiver must use same key during cryptography.



Private Key Method

- **Public-key encryption**: **(two-keys)**

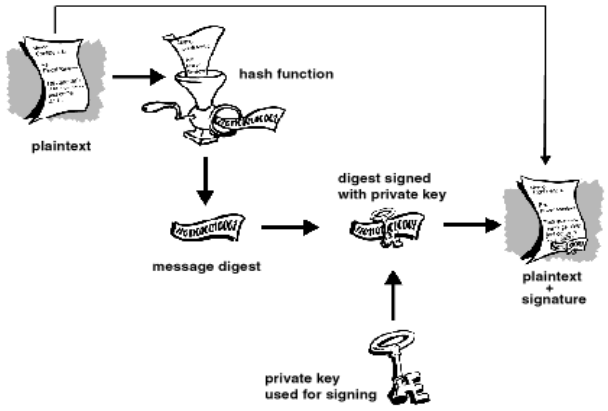
As the name suggest two keys are used one for encryption and other for decryption. Public key and private key are used in this encryption. Public key distributed to any one used for encryption while private key is not distributed to any one and used for decryption. The data is encrypted by public key that decrypted by only private key. Here user using two keys so it is also known as asymmetric key encryption.



From the above figures it can be observed that Encryption is done with Public Key and Decryption with another key called Private Key. This is called **Public key Cryptography**.

- *Hash functions***:**

Hash functions takes large string converted into fixed size length string. Hash function returns value known as message digests and one-way encryption, are algorithms use no key.. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.



III. CRYPTOGRAPHIC TECHNOLOGIES

Based on Layers

- Link layer encryption
- Network layer encryption
- IPSEC, VPN, SKIP
- Transport layer
- SSL, PCT (Private Communication Technology)
- Application layer
- PEM (Privacy Enhanced Mail)
- PGP (Pretty Good Privacy)
- SHTTP

Based on Algorithms

Secret-key encryption algorithms (Symmetric algorithms)

- for encrypt the data DES (Data Encryption Standard) uses 56 bit key.
- Triple DES uses112 bit key for encryption.
- IDEA (International Data Encryption Algorithm) used 128bit key.

Public-key encryption algorithms (Asymmetric algorithms)

- **Diffie-Hellman (DH)**: it is sed for exchanging the keys.
- **RSA:** RSA is used for transmission of data securely. The factorization of the two prime numbers product is very difficult to get.

IV. APPLICATIONS OF CRYPTOGRAPHY

- Defense Services
- Secure Data Manipulation
- E – Commerce
- Business Transactions
- E- Payment Systems
- User Identification Systems
- Access Control
- Computational Security
- Data Security.

V. CONCLUSION

Security is an important aspect in network security . transfer is data more secure manner. In this paper we analysis the different Cryptography algorithms which is used to improve security

REFERENCES.

[1] “Computer Networks” by Andrew S. Tanenbaum,
[2] “Fighting Steganography detection” by Fabian Hansmann,
[3] “Network security” by Andrew S.Tanenbaum,
[4] “Applied Cryptography” by Bruce Schneier, John Willey and Sons Inc,
[5] URL:http://www.woodmann.com/fravia/fabian2.htm.
[6] URL:http://www.jjtc.com/stegdoc/sec202.html