Cryptography-A Security System

Ms Jyoti
M.Tech Student
School of Engineering & Sciences,B P S Mahila Vishwavidayalaya, Sonipat Haryana
Email: happymalik909@gmail.com

----------**ABSTRACT**----------
Network security has become a more practical issue. It basically deals with prevention and monitor of illegal access alternation or incorrect use of the computer network and the resources which are accessible to network. Cryptographic provide network security. It is a science which deals with encryption and decryption of data. It is a practice of writing a secret code. It helps in protection of data and also used for user authentication. This paper represents a survey report of the cryptography approach which is used for network security. The paper recapitulates the related work done in the concerned field since cryptography was developed.

KEYWORDS:- ALGORITHMS, DECRYPTION, DIGITAL SIGNATURE, ENCRYPTION PUBLIC KEY

---

1. INTRODUCTION

The word cryptography comes from the Greek words κρυπτο (hidden or secret) and γραφη (writing). Oddly enough, cryptography is the art of secret writing. More generally, people think of cryptography as the art of mangling information into apparent unintelligibility in a manner allowing a secret method of unmangling. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. In this book we will concentrate on the kind of cryptography that

is based on representing information as numbers and mathematically manipulating those numbers. This kind of cryptography can provide other services, such as it means protection of network from unwanted attackers and authorization of access to networks [1].

Network security is provided using antivirus software package which provided protection against viruses, firewalls, by user authentication in which user's accesses. Network using a username and a password [1], [2].

Cryptography is one of the most popular approach which deals with network securities. Cryptography helps in writing a secret code which cannot be read by anyone except the specified recipient. It deals with encryption and decryption using different keys, Individual who

Deal with this field is known as cryptography.

Main objectives of cryptography are:

- **Privacy:** The code cannot be read by anyone except the specified receiver. To all others, it is unreadable.
- **Authentication:** It ensures that the sender and the receiver have to prove one's identity.
- **Integrity:** The message which is received at receiver side should not be altered and should be in original form.

Non-repudiation: it ensures that this particular message is really sent by the sender.

This section of paper are organised as follows: Section 2 represents the encryption and decryption process, section 3 explains different types of cryptography and their pros and cons. Section 4 explains the significance of keys. Section 5 lists the various application of cryptography approach. Section 6 is the conclusion of this paper.

2. ENCRYPTION AND DECRYPTION

In cryptography, the original text which is to be transmitted is called plain text. The plain text is converted into cipher text using a process of encryption. The encryption algorithm which converts plain text to cipher text is called cipher. Decryption is a process which converts cipher text back into the plain text. Figure 1, illustrates the encryption and decryption process [5],[8][1

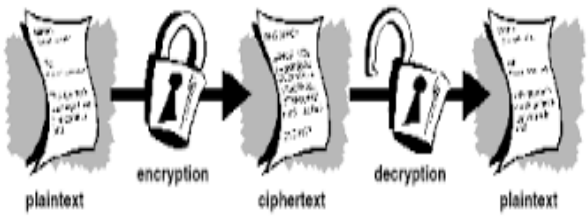

Figure 1: Encryption and Decryption process

3. CRYPTOGRAPHIC ALGORITHMS

For speed, cryptographic algorithms are implemented using hardware and for flexibility, cryptographic algorithms are implemented in software.

The three categories of algorithms are:

- Symmetric algorithms, private key or conventional cryptography.
- Public key cryptography or asymmetric algorithms.
- Hash function algorithms.

Private key Cryptography

In private key cryptography, a single key known as private key is used for both encrypting and decrypting the data. In this, a sender uses a private key to encrypt the data known as plain text to convert it to the cipher text and then, this cipher text is send to the receiver. The receiver uses a same key to decrypt the cipher text and convert it and the original plain text. Since a single key is used for both encryptions, it is also Known as symmetric cryptography. Figure 2 illustrate the public key cryptography process [6]

The various symmetric cryptographic algorithms are:

- DES
- AES
- RCA

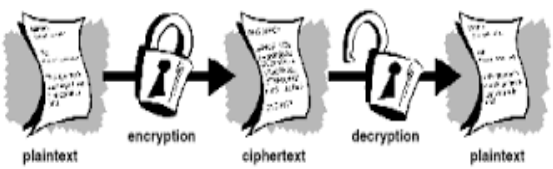

Fig.2: Private key cryptography process

Advantages of Symmetric Cryptography

- They are fast.
- They can process large amount of data.

Disadvantage of Symmetric Cryptography

The main disadvantage is the both sender and receiver should agree on the key and exchange that private key secretly before transmitting the message.

Public key Cryptography

The problems of key distribution are solved by public key cryptography, the concept of which was introduced by Whitfield Diffie and Martin Hellman in 1975. (There is now evidence that the British Secret Service invented it a few years before Diffie and Hellman, but kept it a military secret—and did nothing with it.)1

Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption. You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read.

Since two different keys are used for encryption and decryption of data. it is also known as asymmetric cryptography [4]. The asymmetric cryptographic algorithm is RSA.

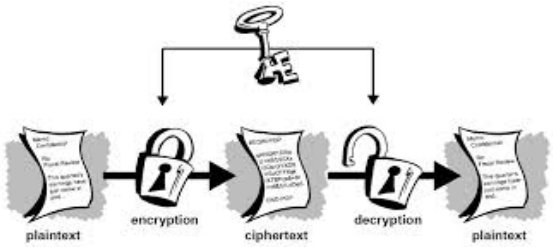

fig.3: Public key cryptography process.

Advantage of public key cryptography

- The sender and receiver can exchange message without meeting each other.
- More secure.
- Private Key is not transmitted.

Disadvantage of public key Cryptography

The main disadvantage of private key cryptography is that it is quite slow.

4. Digital Signatures

Public key cryptography is that it provides a method for employing digital signatures. Digital signatures enable the recipient of information to verify the authenticity of the information's origin, and also verify that the information is intact. Thus, public key digital signatures provide authentication and data integrity. A digital signature also provides non-repudiation.

A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A digital signature is superior to a handwritten signature in that it is nearly impossible to

counterfeit, plus it attests to the contents of the information as well as to the identity of the signer.

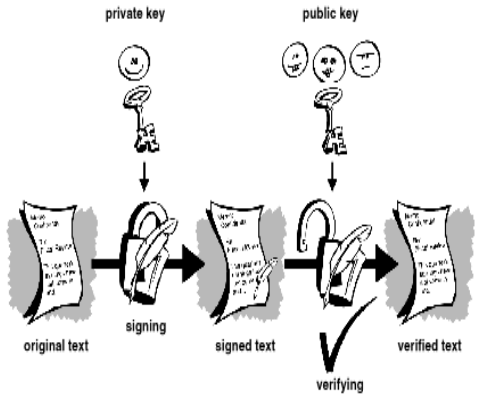

Fig : simple digital signature.

Combination of Private and public key Cryptography

The main disadvantage of public key cryptography is that it is quite slow. So, public key cryptography is used rarely.

a private key algorithm and a key which is made instantly are used by the sender to encrypt the message. Also, sender then encrypts the key known as session key using reviver's public key. Receiver the decrypts the key using its private key to obtain the original session key. now this session key is used to decrypt the message, sender can encrypt the long quickly and send it to the receiver without needing agreement on the session key[8].

5. Hash function

PGP uses a cryptographically strong hash function on the plaintext the user is signing. This generates a fixed-length data item known as a message digest. (Again, any change to the information results in different digest.)

As long as a secure hash function is used, there is no way to take someone's signature from one document and attach it to another, or to alter a signed message in any way. The slightest change in a signed document will cause the digital signature verification process to fail. Hash function is used to check if information is modified or is in original form [6][8].

Two properties of Hash functions are;

- Collision free- The chances that two message will have a same hash value is very small.
- One-way- it is very difficult to find a message whose output hash value matches with a given particular output.

The hash function algorithm is SHA-1.

Advantages of Hash Functions

- it is very easy to compare two messages since the hash value is smaller than the message.
- it is also provide possible to compare two message faster.

6. SIGNIFICANCE OF KEYS

A key is used with cryptographic algorithm.

The security of keys is a must in order to produce a secure cryptographic system. They should be large in size and should be big numbers so, that it becomes difficult to reproduce them. The size of key is measured in bits, it can be 128 bits or 180 bits. the large the key size, more secure is the system. Also, keys should be large in size in order to look for cover time. Cover time is the time required by key is order to protect the data. Keys are encrypted in order to save them. Key rings are the files on hard disk which are used to store keys. It is very difficult to decrypt message.

7. APPLICATIONS OF NETWORK SECURITY-CRYPTOGRAPHY APPROCH

- Military service.
- Data Integrity
- User Authentication.
- User Identification.
- E-Commerce.
- Digital money.
- Data secutity.
- Security of ATM cards.
- Computer passwords.

8. CONCLUSION

Network security is becoming crucial day by day and one of the approaches to provide network security is cryptography. It is very important today. It employs principle of encryption and decryption. There are three types of cryptographic algorithms each having its own pros and cons. The two cryptographic algorithm public key cryptography and private key cryptography can be combined to overcome the problem of speed. It is used to give protection against hackers. Now days, ATM card security is dong through cryptography. Although Cryptography provides high security but 100% security is not achieved even through this.

9. REFERENCES

1. Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone.*Handbook of applied cryptography*. CRC press, 1996.
2. Stallings, William. *Cryptography and Network Security, 4/E*. Pearson Education India, 2006.
3. Koç, Çetin Kaya. *About cryptographic engineering*. Springer US, 2009.
4. Siponen, Mikko T., and Harri Oinas-Kukkonen. "A review of information security issues and respective research contributions." *ACM Sigmis Database* 38, no. 1 (2007): 60-80.
5. Juels, Ari. "RFID security and privacy: A research survey." *Selected Areas in Communications, IEEE Journal on* 24, no. 2 (2006): 381-394.
6. Forouzan, Behrouz A., and Debdeep Mukhopadhyay. *Cryptography And Network Security (Sie)*. McGraw-Hill Education, 2011.

7. Kurtsiefer, Christian, P. Zarda, Matthus Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity. "Quantum cryptography: A step towards global key distribution." *Nature* 419, no. 6906 (2002): 450-450.

8. Dolan, George M., Christopher J. Holloway, and Stephen M. Matyas Jr. "Public key data communications system under control of a portable security device." U.S. Patent 5,604,801, issued February 18, 1997.

1. Abstract line repeating before introduction section.
2. No numbering is provided to Headings in your paper.
3. References in last are bulleted, but numbers are used in citations. How ?