CRYPTOGRAPHY TO SECURE THE COMPUTER NETWORK

Dr. Prashant P. Pittalia

Associate Professor, Department of Computer Science, Gujarat, India

ABSTRACT

Any computer network either it may be home, educational, financial, government or any network it must need a security to protect its devices on the network as well as content within that devices. As the network is not connected with other networks, it is safe but as any of its device connected to the other networks like Internet; it may be affected with the malicious programs and become a vulnerable. In any network either it is intranet or extranet, it having an authentication and authorization service through which it verify and assign the correct resources to the users of the network. This paper describes the cryptography principles and cryptography models and comparisons of cryptographic models.

Keyword: - *Redundancy, Freshness, Public key, Private key*

1. INTRODUCTION

It seems that every other day there is news in communication media about a computer network being compromised by hackers or attackers. At the same time, every organization that uses computer network faces the threat of attack from individuals within the organization. Employees or former employees with who want to obtain credential information or view other employee's contents are also a threat to an organization's computers and networks. Today, computers are most useful if they are networked together to share resources and information. Some precautions are taken by the companies on their computers on a network to reduce the risk of unauthorized access. Every year, financial, healthcare, insurance, corporations, governments, and other organizations spend lots of money on expenditures related to network security. A computer network is a group of computers that are connected to each other so that they may communicate with each other. The internet is the largest network in the world and it is called the network of networks. Through the use of proper hardware and software technologies network security is to be maintained and protect the data and maintain the integrity of the data. Computer and network security is important to protect company assets, to gain a competitive advantage, to smooth functioning of automated system and to provide the services on time. Cryptography is the process to convert the simple text or plain text into the un-interpreted text or encrypted text that could not be understands by the intruders in between the sender and receiver to secure the communication. It deals with developing and analyzing protocols which prevents attackers from retrieving information. Secure communication refers to the scenario where the message or data shared between two parties can't be accessed by intruders. The core principles used in cryptography are Authentication, Data Confidentiality, Data Integrity and Non-repudiation. Authentication verifies the identity of users. The receiver is sure of the sender's identity and that an imposter has not sent the message. Cookies, credit cards, tokens and smart cards, digital certificates are different methods for the authentication. Confidentiality concerns that only the sender and receiver are able to understand the message passing between them. Confidentiality is achieved through the use of cryptosystems, that is, companion encryption and decryption algorithms that respectively lock and unlock the contents of a message. Integrity describes the condition of a message upon receipt, as compared to its original state before transmission. [1]The intermediate parties that handle a message can easily add to, remove from, or modify its contents. Integrity protects the data from unauthorized changes, destruction or damaged. Non-repudiation means the proof that has sent the message. On the internet when any communication happens and if either sender or receiver is deny than non-repudiation helps. The receiver must be able to prove that a received message came from a specific sender. The sender must not be able to deny a sending a message that he/she, in fact, did send.[5]

2. CRYTOGRAPHIC PRINCIPLES

A. Redundancy

It means that all encrypted messages must contain some redundancy, that is, information not needed to understand the message. Also use large size of message.

B. Freshness

It means to add the timestamp in the message to identify either the message is correct one or replay attack. Some method is needed to identify the reply messages. One such measure is including in every message a timestamp valid only for 5 seconds. Then the receiver can keep messages around for 5 seconds, to compare newly arrived messages to previous message to find out duplicates. Messages older than 5 seconds can be rejected, since any replays sent more than 5 seconds later will be rejected as too old. [2]

3. CRYTOGRAPHIC MODELS

There are two cryptographic models known as Symmetric cryptography and Asymmetric cryptography

3.1 Symmetric Key: Cryptography: In symmetric key cryptography the sender uses the key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. In Symmetric key encryption/decryption, the algorithm used for decryption is the inverse of the algorithm used for encryption. This means that if the encryption algorithm uses a combination of addition and multiplication, the decryption algorithm uses a combination of division and subtraction. Here the same key is used for encryption the data and decryption of the data. Before communicating with two parties they must share this key to each other and keep it in secure place to protect against the attacker.

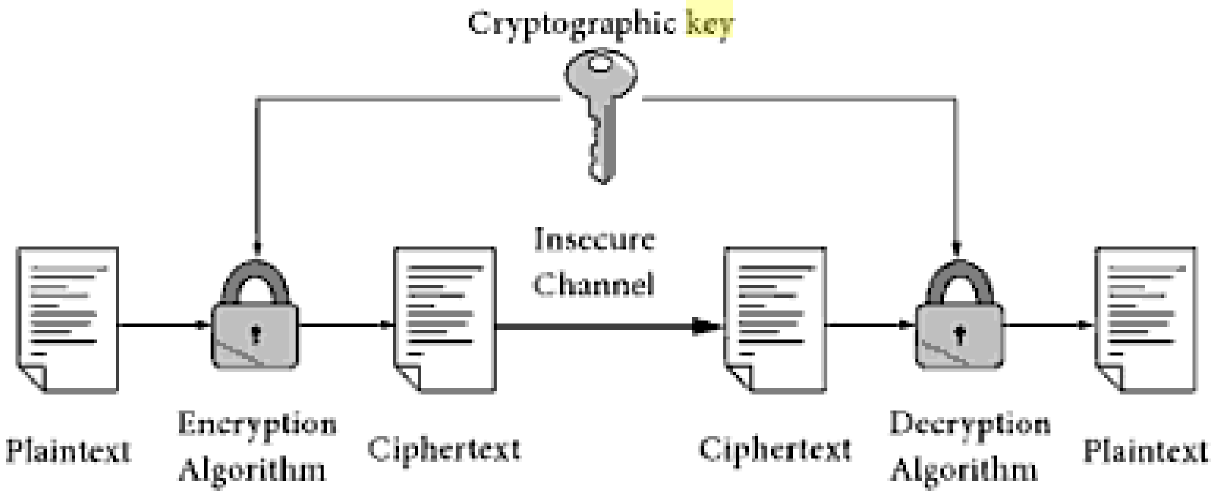

Fig -1: Symmetric Key Cryptography

Advantages:
•It takes less time to encrypt a message using a symmetric key algorithm because the key is smaller.
•It used to encrypt and decrypt long message.
•Cipher text size is same or less than the plain text size.

Disadvantages:
• Each pair of users must have secret key.
•The distribution of the keys between two parties can be difficult.

Symmetric key algorithms are DES (Data Encryption Standard), Tripple-DES (Tripple Data Encryption Standard), AES (Advanced Encryption Standard) RC5 (Rivest Cipher 5), IDEA (International Data Encryption Standard), Blowfish. [3]

3.2 Asymmetric Key Cryptography: In asymmetric key cryptography the two keys are used; a private key and a public key. The receiver keeps the private key. The public key is announced to the public. In asymmetric key encryption/decryption, the public key that is used to encrypt the algorithm is different from the private key that is used to decrypt the algorithm. Each party or node publishes its public key. To provide authentication service, the sender encrypts data with its own private key and sends to the receiver. To decrypt the content and get the original message receiver has to decrypt the data with sender's public key. Same way to provide the confidentiality service in the network , sender encrypt the data or information with the receiver's public key and when such encrypted message reach to destination, receiver decrypt with it's own private key.

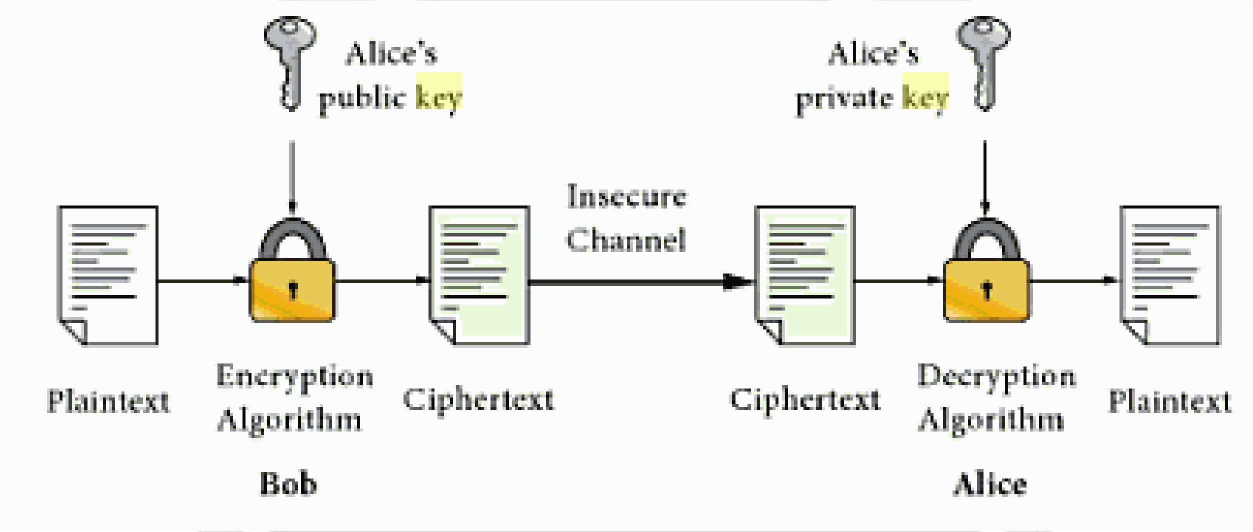

Fig -2: Asymmetric Key Cryptography

Advantages:
•Each entity can create a pair of keys, keep the private one, and publicly distribute the other one.
•Each entity is independent and the pair of keys created can be used to communicate with any other entity.
•It is used for short messages.
•The number of keys needed is reduced.
•In this system, for N users to communicate, only 2N keys are needed.

Disadvantages:
•Complexity of algorithm. Calculating the cipher text from plaintext using the long keys takes a lot of time.
•Cipher text size is more than the plain text size.
•The association between an entity and its public key must be verified. If A sends its public key via an email to B, B must be sure that the public key really belongs to A.

Asymmetric key algorithms are RSA (Rivest-Shamir-Adelman), Diffie-Hellman, ECC (Elliptic Curve Cryptography), EIGamal, DSA (Digital Signature Algorithm). [4]

4. COMPARISION OF CRYTOGRAPHIC MODELS

Symmetric and Asymmetric cryptographic models are compared with the features as Key, Size of encrypted text, speed, Number of keys required, key exchange and usage as below table-1.

Table -1: Comparison of cryptographic models

Characteristic	**Symmetric Key Cryptography**	**Asymmetric Key Cryptography**
Key	Same key is used for encryption & decryption	Public key used for encryption & Private key used for decryption
Size of encrypted text	Same or Less than the plain text size	More than the plain text size
Speed	Very fast	Slower
Number of keys required	N*(N-1)/2 secret keys, so scalability is an issue	2N keys are needed, so scales up quite well
Key exchange	A big problem	No problem at all
Usage	Mainly for encryption and decryption (confidentiality)	Can be used for digital signatures (integrity and non-repudiation checks)

.

5. CONCLUSIONS

Network security is most important component in information security. All information passed through the computer or network or network boundary must be secure with the help of network security software or hardware. A symmetric and asymmetric cryptographic model shows how it helps to protect the corporate networks through the malicious attacks on the network. Also here we compare both the models which give the information that in which situation which model is better to use in network.

6. REFERENCES

[1]. Principles of Computer Security, Fourth Edition,Wm. Arthur Conklin, Greg White, Chuck Cothren, Roger L. Davis, Dwayne Williams,McGraw Hill Professiona

[2]. Cryptographic Protocol: Security Analysis Based on Trusted Freshness, Ling DongKefei ChenJune 20, 2012 Springer Science & Business Media

[3]http://www.omnisecu.com/security/public-key-infrastructure/asymmetric-encryption-algorithms.php

[4] https://en.wikipedia.org/wiki/Symmetric-key_algorithm

[5] Network Security Metrics, Lingyu WangSushil Jajodia Anoop Singhal, November 15, 2017,Springer