Cryptography Algorithms For Providing Security To Data While Transferring Over Network

Jasmin Syed, J S Ananda Kumar

Abstract – Data Security & Cryptography is a concept to protect data while transmission over network. Data Security is the main aspect of secure data transmission over unreliable network. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Data security is involved in organizations, enterprises, and other types of institutions. In this paper we also studied cryptography along with its principles. Cryptographic systems with ciphers are described. The cryptographic models and algorithms are outlined.

Keywords: Information security, Encryption, Decryption, Cryptography, Plain Text, Cipher Text, Keys

1 INTRODUCTION

The main feature of the encryption/decryption program implementation is the generation of the encryption key. Now a day, cryptography has many commercial applications. If we are protecting confidential information then cryptography is provide high level of privacy of individuals and groups. However, the main purpose of the cryptography is used not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation.

Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity.

The Figure 1 shows the classical encryption and the terms in the diagram are defined as:

- **Plaintext**: original message
- **Ciphertext**: coded message
- **Enciphering** or **encryption**: the process of converting from plaintext to ciphertext
- **Deciphering** or **decryption:** the process of restoring the plaintext from the ciphertext

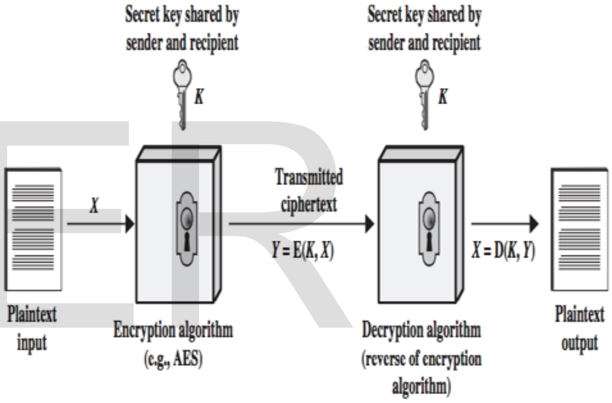
Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 1: Classical Encryption

Security Services:

If we are taking about security of information then following services come in mind.

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)

Jasmin Syed, Lecture, Dept. of DCME, SVEC, Tirupati, Mail id:jasminsyed349@gmail.com.

J S Ananda Kumar, Assistant Professor, Dept .of MCA, KMMIPS, Tirupati, mail id: jsanandkumar@gmail.com.

2 CRYPTOGRAPHIC BASIC PRINCIPLES

A. ***Redundancy***

Cryptographic principle 1: The first principle is that all encrypted messages must contain some redundancy, that is, information not needed to understand the message. Messages must contain some redundancy.

B. ***Freshness***

Cryptographic principle 2: Some method is needed to foil replay attacks. One such measure is including in every message a timestamp valid only for, say, 10 seconds. The receiver can then just keep messages around for 10 seconds, to compare newly arrived messages to previous ones to filter out duplicates. Messages older than 10 seconds can be thrown out, since any replays sent more than 10 seconds later will be rejected as too old.

C. Authentication

Cryptographic principle 3: This is another important principle of cryptographic. In a layman's term, authentication ensures that the message was originated from the originator claimed in the message. Now, one may think how to make it possible? Suppose, Alice sends a message to Bob and now Bob wants proof that the message has been indeed sent by Alice. This can be made possible if Alice performs some action on message that Bob knows only Alice can do. Well, this forms the basic fundamental of Authentication.

D. Integrity

Cryptographic principle 4: Now, one problem that a communication system can face is the loss of integrity of messages being sent from sender to receiver. This means that Cryptography should ensure that the messages that are received by the receiver are not altered anywhere on the communication path. This can be achieved by using the concept of cryptographic hash.

3 TYPES OF CRYPTOGRAPHY

There are several ways of classifying cryptographic techniques. For purposes of this paper, we will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use.

There are three types of cryptography techniques :

i. Secret Key Cryptography

This type of cryptography technique uses just a single key. The sender applies a key to encrypt a message while the receiver applies the same key to decrypt the message. Since only single key is used so we say that this is a symmetric encryption.

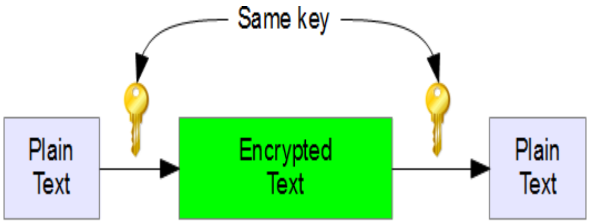

Figure 2: Secrete Key Cryptography

The biggest problem with this technique is the distribution of key as this algorithm makes use of single key for encryption or decryption.

ii. Public Key Cryptography

This type of cryptography technique involves two key crypto system in which a secure communication can take place between receiver and sender over insecure communication channel. Since a pair of keys is applied here so this technique is also known as asymmetric encryption.

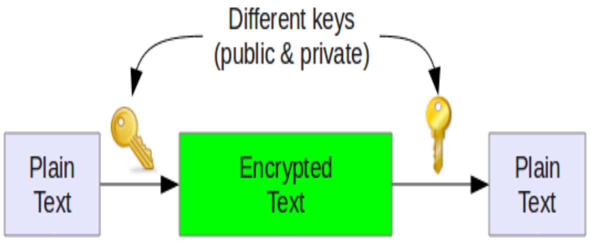

Figure 3: Public Key Cryptography

In this method, each party has a private key and a public key. The private is secret and is not revealed while the public key is shared with all those whom you want to communicate with.

iii. Hash Functions

This technique does not involve any key. Rather it uses a fixed length hash value that is computed on the basis of the plain text message. Hash functions are used to check the integrity of the message to ensure that the message has not be altered, compromised or affected by virus.

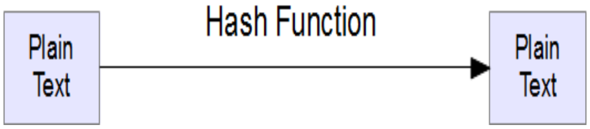

Figure 4: Hash Function

Hash functions, also called *message digests* and *one-way encryption*, are algorithms that, in essence, use no key. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

4 CRYPTOGRAPHIC MODELS

Encryption model There are two encryption models namely they are as follows: Symmetric encryption and Asymmetric encryption.

Symmetric encryption: In this model, Encryption key is equal to Decryption key.

Asymmetric encryption: In this model, Encryption key not equal to Decryption key.

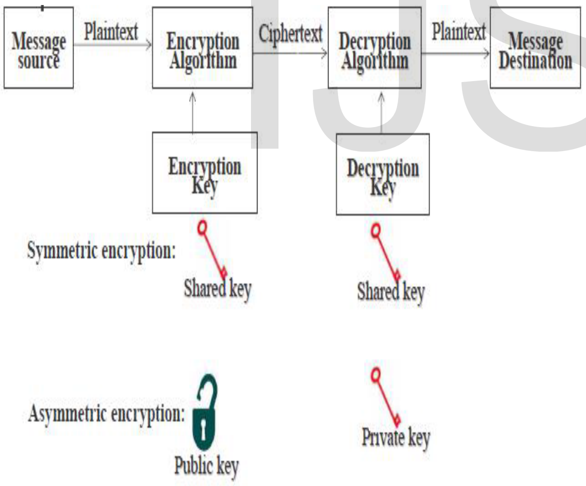

Figure 5: Cryptography

5 CRYPTOGRAPHY ALGORITHMS

There are of course a wide range of cryptographic algorithms in use. The following are amongst the most well-known:

i. *DES:* This is the 'Data Encryption Standard'. This is a cipher that operates on 64-bit blocks of data, using a 56-bit key. It is a 'private key' system. Further Details on the DES Algorithm.

ii. *RSA:* RSA is a public-key system designed by Rivest, Shamir, and Adleman. Further Details on the RSA Algorithm.

iii. *HASH:* A 'hash algorithm' is used for computing a condensed representation of a fixed length message/file. This is sometimes known as a 'message digest', or a 'fingerprint'.

iv. *MD5:* MD5 is a 128 bit message digest function. It was developed by Ron Rivest. Further Details on the MD5 Algorithm.

v. *AES:* This is the Advanced Encryption Standard (using the Rijndael block cipher) approved by NIST.

vi. *Blowfish:* A symmetric 64-bit block cipher invented by Bruce Schneier; optimized for 32-bit processors with large data caches, it is significantly faster than DES on a Pentium/PowerPC-class machine. Key lengths can vary from 32 to 448 bits in length. Blowfish, available freely and intended as a substitute for DES or IDEA, is in use in a large number of products.

vii. *Twofish:* A 128-bit block cipher using 128-, 192-, or 256-bit keys. Designed to be highly secure and highly flexible, well-suited for large microprocessors, 8-bit smart card microprocessors, and dedicated hardware. Designed by a team led by Bruce Schneier and was one of the Round 2 algorithms in the AES process.

viii. *SHA-1:* SHA-1 is a hashing algorithm similar in structure to MD5, but producing a digest of 160 bits (20 bytes).Because of the large digest size, it is less likely that two different messages will have the same SHA-1 message digest. For this reason SHA-1 is recommended in preference to MD5.

ix. *CAST-128/256:* CAST-128, described in Request for Comments (RFC) 2144, is a DES-like substitution-permutation crypto algorithm, employing a 128-bit key operating on a 64-bit block. CAST-256 (RFC 2612) is an extension of CAST-128, using a 128-bit block size and a variable length (128, 160, 192, 224, or 256 bit) key. CAST is named for its developers, Carlisle Adams and Stafford Tavares, and is available internationally. CAST-256 was one of the Round 1 algorithms in the AES process.

x. *International Data Encryption Algorithm (IDEA):* Secret-key cryptosystem written by Xuejia Lai and James Massey, in 1992 and patented by Ascom; a

64-bit SKC block cipher using a 128-bit key. Also available internationally.

xi. *HMAC:* HMAC is a hashing method that uses a key in conjunction with an algorithm such as MD5 or SHA-1. Thus one can refer to HMAC-MD5 and HMAC-SHA1.

xii. *Rivest Ciphers (*aka *Ron's Code):* Named for Ron Rivest, a series of SKC algorithms.

   a. *RC1:* Designed on paper but never implemented.

   b. *RC2:* A 64-bit block cipher using variable-sized keys designed to replace DES. It's code has not been made public although many companies have licensed RC2 for use in their products. Described in RFC 2268.

   c. *RC5:* A block-cipher supporting a variety of block sizes (32, 64, or 128 bits), key sizes, and number of encryption passes over the data. Described in RFC 2040.

   d. *RC6:* A 128-bit block cipher based upon, and an improvement over, RC5; RC6 was one of the AES Round 2 algorithms.

xiii. *KCipher-2:* Described in RFC 7008, KCipher-2 is a stream cipher with a 128-bit key and a 128-bit initialization vector. Using simple arithmetic operations, the algorithms offers fast encryption and decryption by use of efficient implementations. KCipher-2 has been used for industrial applications, especially for mobile health monitoring and diagnostic services in Japan.

xiv. *Tiny Encryption Algorithm (TEA):* A family of block ciphers developed by Roger Needham and David Wheeler. TEA was originally developed in 1994, and employed a 128-bit key, 64-bit block, and 64 rounds of operation.

xv. *GSM (Global System for Mobile Communications, originally Groupe Spécial Mobile) encryption:* GSM mobile phone systems use several stream ciphers for over-the-air communication privacy.

xvi. *HAVAL (HAsh of VAriable Length):* Designed by Y. Zheng, J. Pieprzyk and J. Seberry, a hash algorithm with many levels of security. HAVAL can create hash values that are 128, 160, 192, 224, or 256 bits in length.

xvii. *Tiger:* Designed by Ross Anderson and Eli Biham, Tiger is designed to be secure, run efficiently on 64-bit processors, and easily replace MD4, MD5, SHA and SHA-1 in other applications. Tiger/192 produces a 192-bit output and is compatible with 64-bit architectures; Tiger/128 and Tiger/160 produce a hash of length 128 and 160 bits

6 CONCLUSION

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together. We have studied various cryptographic techniques to increase the security of network. Cryptography, together with suitable communication protocols, can provide a high degree of protection in digital communications against intruder attacks as far as the communication between two different computers is concerned.

REFERENCES

[1] DENNING, D., and DENNING, P.J.: 'Data security', *ACM Comput. Surveys*, 1979, 11, pp. 227-250

[2] A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco.

[3] Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.

[4] 'Data encyption standard', FIPS PUB 46, National Bureau of Standards,Washington, DC Jan. 1977

[5] Murat Fiskiran , Ruby B. Lee, ―Workload Characterization of Elliptic Curve Cryptography and other Network Security Algorithms for Constrained Environments‖, IEEE International Workshop on Workload Characterization, 2002. WWC-5. 2002.

[6] Coron, J. S. , " What is cryptography?", *IEEE Security & Privacy Journal, 12(8), 2006, p. 70-73.*

[7] Pfleeger, C. P., & Pfleeger, S. L.," *Security in Computing"*, Upper Saddle River, NJ: Prentice Hall.2003.

[8] Salomon, D., " *Coding for Data and Computer Communications"*, New York, NY: Spring Science and Business Media. 2005.

[9] Shannon, E. C., "Communication theory of secrecy system", *Bell System Technical Journal,* Vol.28, No.4, 1949, pp.656- 715.

[10]DIFFIE, W., and HELLMAN, M.: 'New directions in cryptography', *IEEE Trans.*, 1976, **IT-22,** pp. 644-654

[11] SIMMONS, G.J.: 'Symmetric and asymmetric encryption', *ACM Comput. Surveys,* 1979, **11,** pp. 305-330

[12] RIVEST, R.L., SHAMIR, A., and ADLEMAN, L: 'A method for obtaining digital signatures and public-key cryptosystems', *CACM,* 1978, **21,** pp. 120-126

[13]Algorithms:
http://www.garykessler.net/library/crypto.html#