International Journal of IT & Knowledge Management (ISSN: 0973-4414)
July-Dec 2008, Vol 1, Number-2, pp 568-570

IMPORTANCE OF CRYPTOGRAPHY IN NETWORK SECURITY

[1]Dr.S.Thajoddin, [2]S.Makbul Hussian, [3]Dr.SAM Gazni

[1,2] Lecturer in Mathematics, Dept. of Mathematics, [3]Lecturer in Physics, Dept. of Physics

[1,2,3]Osmania College , Kurnool AP, India

Abstract: Cryptography is the science of writing the data or information in a secret code.It includes techniques such as microdots, merging words with images and other ways to hide information in storage or transit. The cryptographic schemes works on the basis of some mathematical algorithms along with a key. This key is being used for encryption as well as for the decryption of the data. In secret key cryptography, the same key is used for both the encryption as well as the decryption of the messages. In PKC, a pair of different keys is used; one key is used for encryption and another decryption key for decryption.

Key words: Cryptography, secret key, PKC, encryption, decryption.

1.1. INTRODUCTION :

The world is becoming more interconnected with the advent of the internet and new networking technologies .There is a large amount of personal commercial, military and government information on networking infrastructures worldwide. This information is of great importance because which is the intellectual property that can be easily acquired through the internet. But rapidly raising cyber crimes and the growing prospects of the internet being used as a medium for terrorist attacks pose a major challenge for information security. And that is where the need for cryptography arises.

Cryptography is the science of writing the data or information in a secret code. It includes techniques such as microdots, merging words with images and other ways to hide information in storage or transit. However in today's computer centric world, cryptography is most often associated with encryption and decryption. The data that can be understood easily without any special efforts is called as the plain text. This data can be converted into the secret code and this process is called as the encryption. This encrypted data is called as the cipher text.

This cipher text can convert back into the plain text (by a key) and this process is called as the decryption. Thus cryptography consists of the both the encryption and the decryption process.

1.2 OBJECTIVES OF CRYPTOGRAPHY

Cryptography concerns itself with the following four objectives

a) CONFIDENTIALITY: The information cannot be understood by anyone for whom it was unintended.

b) INTEGERITY: The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

c) NON REPUDICATION: The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

d) AUTHENTICATION: The sender and receiver can confirm each other's identity and the origin /destination of the information.

1.3 WORKING OF CRYPTOGRAPHY

The cryptographic schemes works on the basis of some mathematical algorithms along with a key. This key is being used for encryption as well as for the decryption of the data. The key used for these two processes can be either same or it can be different as well as in various different types of cryptography.

1.4 TYPES OF CRYPTOGRAPHY

There are three general types of cryptographic schemes.

1. Secret key cryptography or symmetric cryptography.
2. Public key cryptography or symmetric cryptography.
3. Hash functions.

However, public key cryptographic schemes are more important than other two. So we pay particular attention on public key cryptosystems.

1.4.1 SECRET KEY CRYPTOGRAPHY: [SKC]

In secret key cryptography, the same key is used for both the encryption as well as the decryption of the messages. In this scheme, the sender uses the key to encrypt the plain text and sends the cipher text to the receiver. The receiver applies the same key to descript the message and recovers the plain text. Because a single key is used for the both functions, secret key cryptography is also called symmetric encryption. With thin form of cryptography, it is obvious that the key must be known to both the sender and receiver, that, in fact, is the secret .The biggest difficulty with this scheme, of course, is the distribution of the key .The most common secret key cryptography scheme used today is DES (Data Encryption Standard)

1.4.2 PUBLIC KEY CRYPTOGRAPHY [PKC]

In PKC, a pair of different keys is used, one key is used for encryption and another key for decryption.

Generic PKC employees two keys that are mathematically related, although knowledge of one key does not allow someone to easily determine the other key. One key is used to encrypt the plain text and other key is used to decrypt the cipher text. The important point here is that it doesn't matter which key is applied first, but that both keys are required for the process to work. Because a pair of keys' is required, this approach is called as asymmetric cryptography.

In PKC, one of the keys is designated the public key may be advertised as widely as the owner wants. The other key is designated as the private key and it is never revealed to another party. It is straight forward to send messages under these schemes. Suppose Alice wants to send Bob a message. Alice encrypts some information using Bob's public key. Bob decrypt the cipher text using his private key.

The public key cryptographic algorithms that are in common use today are

1. RSA Algorithm
2. Diffie – Hellman key exchange
3. T.El Gamal algorithm
4. Paillier cryptosystem

1.4.3 USES OF PUBLIC KEY CRYPTOSYSTEMS

There are two main uses for public key cryptography

1. PUBLIC KEY ENCRYPTIONS :

In public key encryption, a message is encrypted with a recipient's public key. The message cannot be decrypted by anyone who doesn't possess the matching private key, who is thus presumed to be owner of that key and the person associated with the public key. This is used in an attempt to ensure confidentially.

2. DIGITAL SIGNATURES :

In digital signatures, a message is signed with the sender's private key and can be verified by anyone who has access to the sender's public key. This verification proves that sender had access to the private key, and therefore is likely be the person associated with the public key. This also ensures that the messages has not been tampered, as any manipulation of the message will results in changes to the encoded message digest, which otherwise remains unchanged between the sender and receivers .

1.4.4 HASH FUNCTIONS:

Hash functions are mathematical computations that take in a relatively arbitrary amount of data as input and produce an output of fixed size. The output is always the same when given the same input. The inputs to a Hash functions are typically called messages, and the outputs often refer to as message digest. Nearly any piece of data can be defined as a message including character strings, binary files and TCP packets. The popular Hash functions used today are MD5 (message digest 5) and SHA1 (secure hash algorithm 1).

CONCLUSION: Cryptography is the most common and important for providing network security. In Cryptography public key cryptography is the most significant development and it is the basic stuff from which we make street lights for the information high way. Cryptography provides a bundles extremely fundamental services , authentication , privacy message integrity and non repudiation among others . It is one of the basic building blocks for computer network.

REFERENCES

1) A.J. Menezes, P.C.Van Oorschot and S.A.Vanstone : Handbook of Applied Cryptography, CRC Press, 1996
2) D.R. Stinson : Cryptography Theory and Practice, CRC 1995
3) G.J. Simmons: Contemporary Cryptography: The science of information integrity, IEEE Press, 1992.
4) Stallings W.Cryptography and Network security. Upper Saddle River, NJ : Prentice Hall, 2006.
5) Rhee, M.Internet Security, Hoboken, NJ: John Wiley & Sons, 2003
6) Solomon, D.Data Privacy and security, Berlin : Springer 2003.
7) Trappe W and Washington L Introduction to cryptography and coding theory. Upper Saddle River, NJ : Prectice Hall, 2006.
8) Preprzyk, J.Hardjono I, and Seberry J.Fundmentals of Computer security Berlin : Springer, 2003.
9) Mao.W.Modrn Cryptography, Upper Saddle River, NJ: Practice Hall 2004.
10) Kanfman, C.Perlman, R. and Specimer, M.Network Security, Upper Saddla River, NJ : Practice Hall, 2004.
11) Menezes.A. Oorschot.P, and Vanstone, S.Handbook of applied cryptography. Newyork CRC press, 1997.