IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

NETWORK SECURITY AND CRYPTOGRAPHY

Prof. Pavitra M. Gadhar1, Pooja M. Shindhe2*

Assistant Professor1, Student2*

Department of Computer Science & Engineering

R.T.E Society's Rural Engineering College Hulkoti - 582205India

Abstract

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become "wired", an increasing number of people need to understand the basics of security in a networked world. This document was written with the basic computer user and information systems manager in mind, explaining the concepts needed to read through the hype in the marketplace and understand risks and how to deal with them. So it is very important for all the users to get familiar with various aspects of Network Security. In the article basics of Network Security are discussed. With the millions of Internet users able to pass information from the network, the security of business networks is a major concern. The very nature of the Internet makes it vulnerable to attack. The hackers and virus writers try to attack the Internet and computers connected to the Internet. With the growth in business use of the Internet, network security is rapidly becoming crucial to the development of the Internet. Many business set up firewalls to control access to their networks by persons using the Internet.

This paper aims to provide a broad review of **network security and cryptography**. Network security and cryptography is a subject too wide ranging to coverage about how to protect information in digital form and to provide security services. However, a general overview of network security and cryptography is provided.

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. When many systems are connected in a network it is very important to safeguard the data in each system. However, as more and more people become "wired", an increasing number of people need to understand the basics of security in a networked world. Our paper covers different kinds of threats & firewalls in the network by implementation of different security services using various security mechanisms. Generally, the logical conclusion is to use both kind of algorithms and their combinations to achieve optimal speed and security levels. It is hoped that the reader will have a wider perspective on security in general, and better understand how to reduce and manage risk personally.

INTRODUCTION

Network security deals with the problems of legitimate messages being captured and replayed. Network security is the effort to create a secure computing platform. The action in question can be reduced to operations of access, modification and deletion. Many people pay great amounts of lip service to security, but do not want to be bothered with it when it gets in their way. It's important to build systems and networks in such a way that the user is not constantly reminded of the security system. Users who find security policies and systems to restrictive will find ways around them. It's important to get their feed back to understand what can be improved, the sorts of risks that are deemed unacceptable, and what has been done to minimize the organizations exposure to them.

Network security problems can be divided roughly into four intertwined areas: **secrecy, authentication, nonrepudiation,** and **integrity control.**

- Secrecy has to do with keeping information out of the hands of unauthorized users.
- Authentication deals with whom you're talking to before revealing sensitive information or entering into a business deal.
- No repudiation deals with signatures.
- Integrity control deals with long enterprises like banking, online networking.

CRYPTOGRAPHY

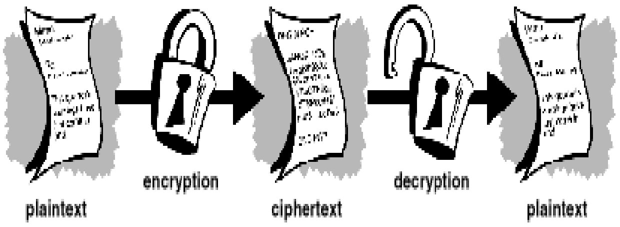
The term cryptology has its origin in Greek kryptos logos, which means "hidden word." Cryptography is the science of protecting data.

➢ Cryptography Process:

- **Plain text**: The messages to be encrypted known as plain text or clear text.
- **Encryption**: The process of producing cipher text is called Encryption.

These problems can be handled by using cryptography, which provides means and methods of converting data into unreadable form, so that **Valid User** can access Information at the Destination.

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet, mobiles) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Cryptanalysts are also called **attackers**. Cryptology embraces both cryptography and cryptanalysis.



Cryptography process

- **Cipher text**: Encrypted message is called cipher text.
- **Decryption**: The process of retrieving the plain text from the_cipher text is called decryption.

Encryption and decryption usually make use of a **key**, i.e. the messages to be encrypted are transformed by a function that is parameterized by a key. The art of breaking ciphers is called **cryptanalysis**.

The art of devising ciphers (**cryptography**) and breaking them (**cryptanalysis**) is collectively known as **cryptology**.

- **Fundamental Requirements:**

- **Confidential:** Is the process of keeping information private and Secret so that only the intended recipient is able to understand the information.
- **Authentication:** 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 is who and what he or she claims to be.
- **Integrity:** Is the method to ensure that information is not tampered with during its transit or its storage on the network. Any unauthorized person should not be able to tamper with the information or change the Information during transit
- **Non-repudiation:** Is the method to ensure that information cannot be disowned. Once the non-repudiation process is in place, the sender cannot deny being the originator of the data.
- **Access control**: Requires that access to information resources may be controlled for target system.
- **Availability:**The availability of computer systems must be only for authorized parties when ever needed.

- **Security Attacks**:

- **Interruption:** In an attack where one or more of the systems of the organization become unusable due to attacks by unauthorized users. This leads to systems being unavailable for use.
- **Interception:** An unauthorized individual intercepts the message content and changes it or uses it for malicious purposes. After this type of attack, the message does not remain confidential.
- **Modification:** The content of the message is modified by a third party. This attack affects the integrity of the message.

So for maintaining the data secretly while communicating data between two persons or two organizations data is to be converted to other format and the data is to be transmitted. So now we deal with the Cryptography, which is process of transmitting data securely without any interruption. Network security is the security of data transmission in the communication.

- **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'

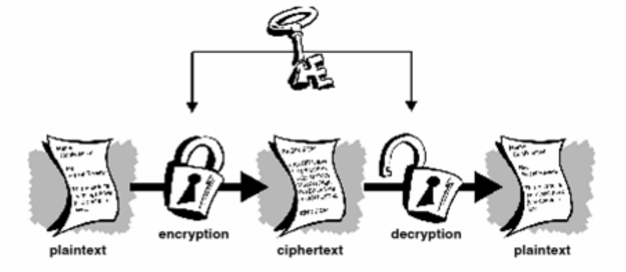
Original Plaintext—M

Decryption function—D

Encryption function—E

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

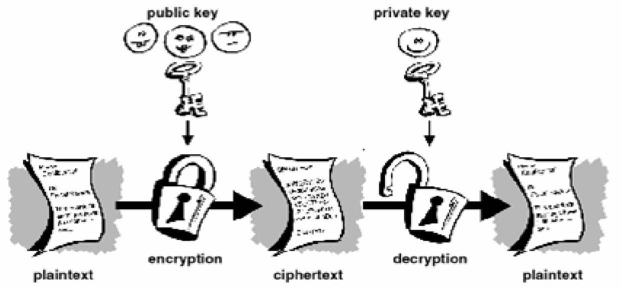
Symmetric-key encryption, also called shared-key encryption or **secret-key cryptography** (**Private-key method**), uses a single key that both the sender and recipient possess. This key, used for both encryption and decryption, is called a **secret key** (also referred to as a symmetric key or session key). Symmetric-key encryption is an efficient method for encrypting large amounts of data. But the drawback is to transfer the Key to Receiver, as it is prone to security risks.



Private Key Method

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

Two keys—a **public key** and a **private key**, which are mathematically related—are used in public-key encryption. To contrast it with symmetric-key encryption, public-key encryption is also sometimes called **asymmetric-key encryption**. In public-key encryption, the public key can be passed openly between the parties or published in a public repository, but the related private key remains private. Data encrypted with the public key can be decrypted only using the private key. Data encrypted with the private key can be decrypted only using the public key. In the below figure, a sender has the receiver's public key and uses it to encrypt a message, but only the receiver has the related private key used to decrypt the message.

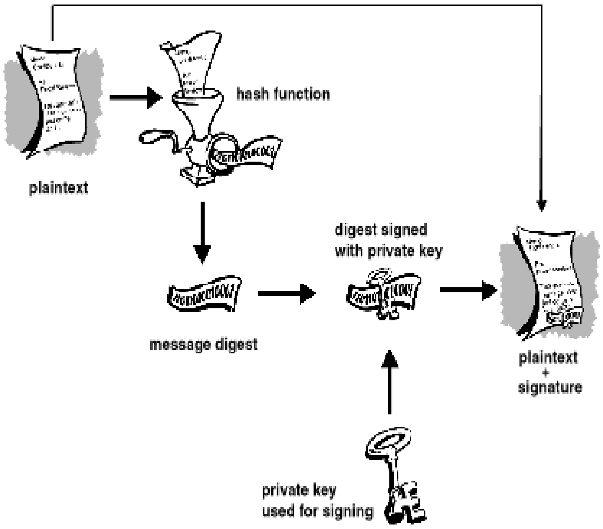


Public Key Method

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:**

An improvement on the Public Key scheme is the addition of a one-way hash function in the process. A one-way hash function takes variable length input. In this case, a message of any length, even thousands or millions of bits and produces a fixed-length output; say, 160-bits. The hash function ensures that, if the information is changed in any way even by just one bit an entirely different output value is produced. 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 Functions

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

Cryptographic process can be implemented at various layers starting from the link Layer all the way up to the application layer. The most popular encryption scheme is SSL and it is implemented at the transport layer. If the encryption is done at the transport layer, any application that is running on the top of the transport layer can be protected.

Based on Algorithms

Secret-key encryption algorithms (Symmetric algorithms)

- DES (Data Encryption Standard) -- 56 bit key
- Triple DES --112 bit key
- IDEA (International Data Encryption Algorithm) --128bit key

Public-key encryption algorithms (Asymmetric algorithms)

- **Diffie-Hellman (DH)**: Exponentiation is easy but computing discrete logarithms from the resulting value is practically impossible.
- **RSA:** Multiplication of two large prime numbers is easy but factoring the resulting product is practically impossible

APPLICATIONS OF CRYPTOGRAPHY

- Defense Services
- Secure Data Manipulation
- E – Commerce
- Business Transactions
- Internet Payment Systems
- Pass Phrasing Secure Internet Comm.
- User Identification Systems
- Access Control
- Computational Security
- Secure access to Corp Data
- Data Security

APPLICATIONS OF NETWORK SECURITY

Computer networks were primarily used by university researchers for sending email, and by corporate employees for sharing printers. Under these conditions, security did not get a lot of attention. But now, as millions of ordinary citizens are using networks for:

- Banking
- Shopping
- Filling their tax returns.

CONCLUSION

Network security is a very difficult topic. Everyone has a different idea of what “security” is, and what levels of risk are acceptable. The key for building a secure network is to define what security means to your organization. Once that has been defined, everything that goes on with. The network can be evaluated with respect to the policy. Projects and systems can then be broken down into their components, and it becomes much simpler to decide whether what is proposed will conflict with your security policies and practices.

Security is everybody’s business, and only with everyone’s cooperation, intelligent policy, and consistent practices, will it be achievable.

Cryptography protects users by providing functionality for the encryption of data and authentication of other users. This technology lets the receiver of an electronic message verify the sender, ensures that a message can be read only by the intended person, and assures the recipient that a message has not be altered in transit. The Cryptography Attacking techniques like Cryptanalysis and Brute Force Attack. This Paper provides information of Advance Cryptography Techniques.

BIBOLOGRAPHY

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.html.
6. URL:http://www.jjtc.comstegdoc/sec202.html