NETWORK SECURITY

6th Semester

By:- Deepak Rohilla

Importance of Network Security

The purpose of network security is essentially to prevent loss, through misuse of data. There are a number of potential pitfalls that may arise if network security is not implemented properly. Some of these are:

- **Breaches of confidentiality**: Each business will identify with the need to keep certain critical information private from competitor eyes.

Cont……..

Importance of Network Security

- **Data destruction**: Data is a very valuable commodity for individuals and enterprises alike

- **Data manipulation**: Data manipulation is a more insidious threat.

Implementing Network Security

- The best approach to implementing a good network security strategy is to be well-prepared for attacks. There is a four-step process:
  - **Secure**: Ensure that all the components are well-guarded with adequate authentication and authorization policies.
  - **Examine:** Constantly monitor network activity and safeguards erected.
  - **Test:** Assess the vulnerabilities of network security policies by having them attacked by a trusted entity. If the safeguards can be breached, it is time to implement more stringent techniques.
  - **Enhance:** Based on all the preceding phases, collect data and use it to build better safeguards.

Principles of Security

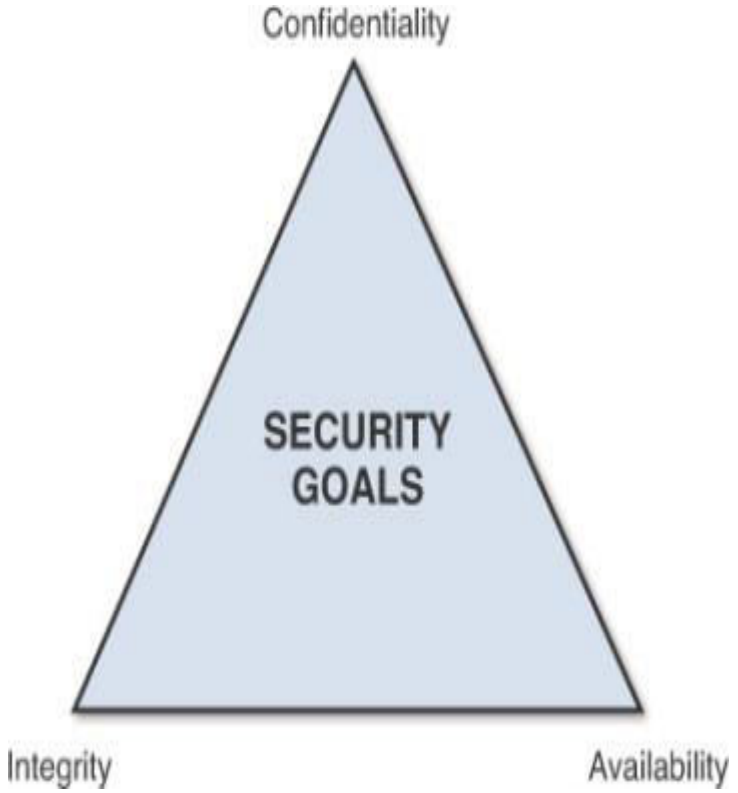
The principle of information security is protection of **Confidentiality, Integrity,** and **Availability** cannot be overemphasized:

All information security measures try to address at least one of three goals:

- Protect the confidentiality of data
- Preserve the integrity of data
- Promote the availability of data for authorized use

The CIA triad

- These goals form the confidentiality, integrity, availability (CIA) triad, the basis of all security programs . Information security professionals who create policies and procedures (often referred to as governance models) must consider each goal when creating a plan to protect a computer system.



Types of attack

An attack can be *active* or *passive*.

- An "**active attack**" attempts to alter system resources or affect their operation.
- A "**passive attack**" attempts to learn or make use of information from the system but does not affect system resources.

External and Internal Threats

- An **external security threat** occurs when someone outside your network creates a security threat to your network. If you are using an intrusion-detection system (IDS), which detects attacks as they occur, you probably will be mildly shocked at the number of probes and attacks that occur against your network daily.
- An **internal security threat** occurs when someone from inside your network creates a security threat to your network.

Unstructured and Structured Threats

- An unstructured security threat is one created by an inexperienced person who is trying to gain access to your network.
- A structured security threat, on the other hand, is implemented by a technically skilled person who is trying to gain access to your network.

Cybercrime

- **Cybercrime**, also called computer crime, is any illegal activity that involves a computer or network-connected device, such as a mobile phone.

Cybercrime categories

The Department of Justice divides cybercrime into three categories:

1. Crimes in which the computing device is the target, for example, to gain network access;
2. Crimes in which the computer is used as a weapon, for example, to launch a denial of service (DoS) attack;
3. Crimes in which the computer is used as an accessory to a crime, for example, using a computer to store illegally-obtained data.

Cyberethics

Cyberethics is the philosophic study of ethics pertaining to computers, encompassing user behaviour and what computers are programmed to do, and how this affects individuals and society.

What is hacking

- Hacking is the practice of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose. The person who is consistently engaging in hacking activities, and has accepted hacking as a lifestyle and philosophy of their choice, is called a hacker.

Types of Hackers

- **Ethical Hacker:-** A hacker who gains access to systems with a view to fix the identified weaknesses.
- **Cracker:-** A hacker who gains unauthorized access to computer systems for personal gain.
- **Script kiddies:-** A non-skilled person who gains access to computer systems using already made tools
- **Hacktivist:** A hacker who use hacking to send social, religious, and political etc. messages.
- **Phreaker:** A hacker who identifies and exploits weaknesses in telephones instead of computers.

Ethical hacking

- **Ethical hacking** and **ethical hacker** are terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network. This information is then used by the organization to improve the system security, in an effort to minimize or eliminate any potential attacks.

Securing Data over Internet

ENCRYPTION AND DECRYPTION

Plaintext: -Data that can be read and understood without any special measures is called plaintext or cleartext.

Encryption :- The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext.

Decryption :-The process of reverting ciphertext to its original plaintext is called decryption

Cryptography

- 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) so that it cannot be read by anyone except the intended recipient.

Five primary functions of cryptography

- ***Privacy/confidentiality***: Ensuring that no one can read the message except the intended receiver.
- ***Authentication:*** The process of proving one's identity.
- ***Integrity:*** Assuring the receiver that the received message has not been altered in any way from the original.
- **Non-repudiation:** A mechanism to prove that the sender really sent this message.
- **Key exchange:** The method by which crypto keys are shared between sender and receiver.

TYPES OF CRYPTOGRAPHIC ALGORITHMS

- ***Secret Key Cryptography*** *(SKC)*: Uses a single key for both encryption and decryption; also called *symmetric encryption*. Primarily used for privacy and confidentiality.

A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

Cont…….

TYPES OF CRYPTOGRAPHIC ALGORITHMS

- ***Public Key Cryptography*** *(PKC)*: Uses one key for encryption and another for decryption; also called *asymmetric encryption*. Primarily used for authentication, non-repudiation, and key exchange.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

Cont…….

TYPES OF CRYPTOGRAPHIC ALGORITHMS

- ***Hash Functions***: Uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. Primarily used for message integrity (Message integrity means that a message has not been tampered with or altered i.e validity of a transmitted message) .

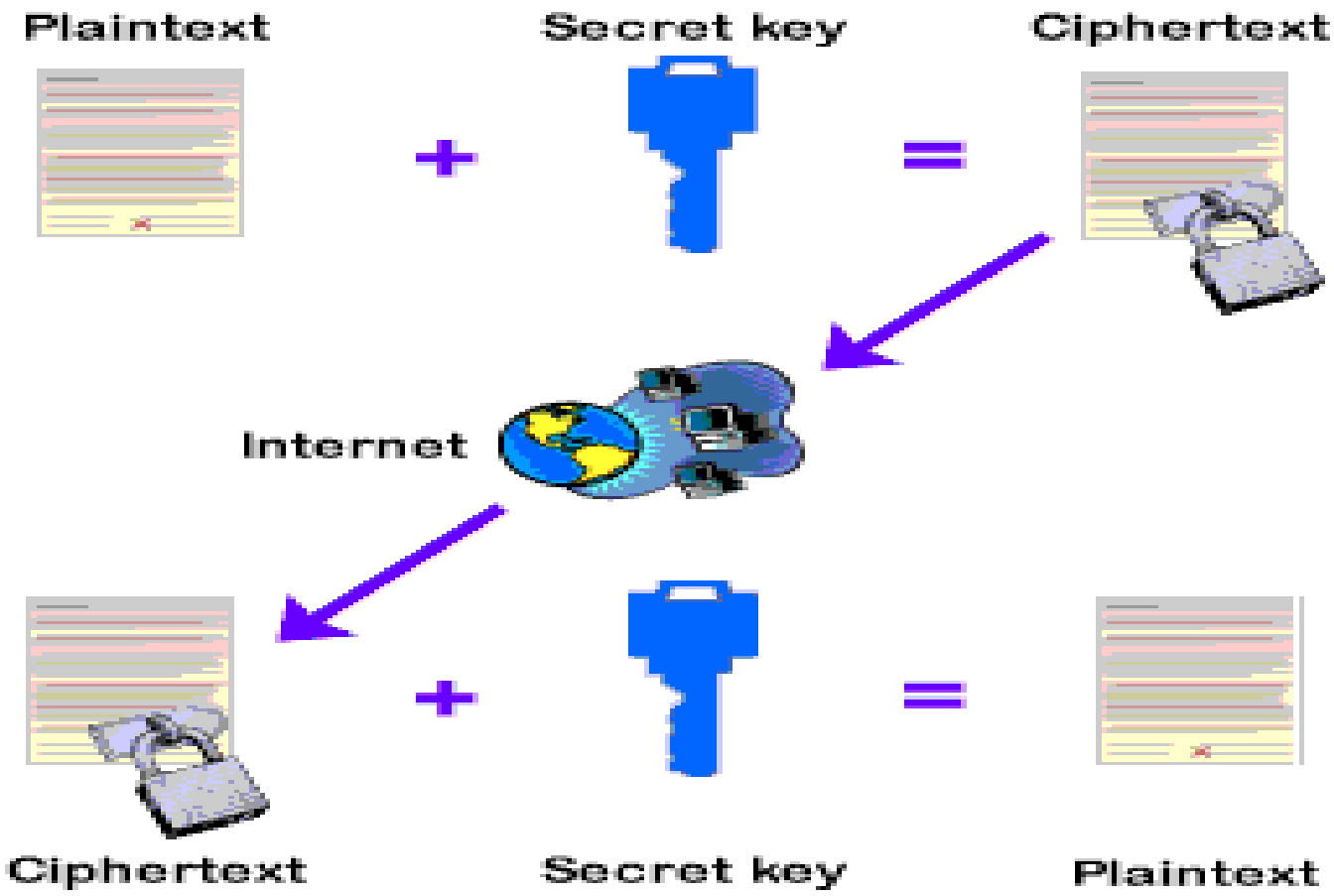
C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Symmetric key algorithms (Private key cryptography)

- Both parties share a private key (kept secret between them).
- Symmetric key algorithms are what you use for encryption. For example: encryption of traffic between a server and client, as well as encryption of data on a disk.

Cont……

Symmetric key algorithms (Private key cryptography)



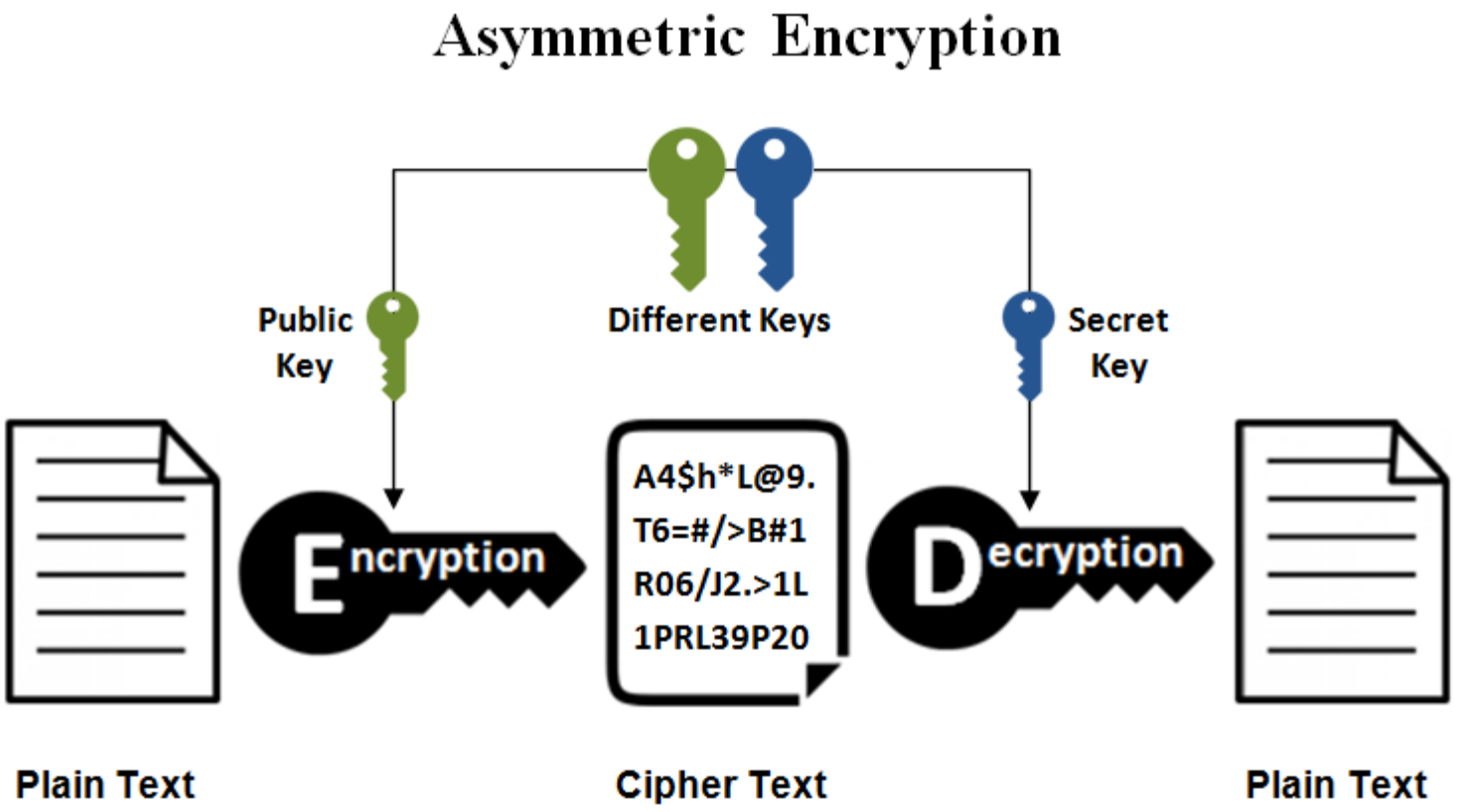
Asymmetric key algorithms (Public key cryptography)

- Asymmetric cryptography is a branch of cryptography where a secret key can be divided into two parts, a public key and a private key.

  One key in the pair can be shared with everyone; it is called the **public key**. The other key in the pair is kept secret; it is called the **private key**. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

Cont……

Symmetric key algorithms (Private key cryptography)



RSA – short for the surnames of its designers (Rivest, Shamir and Adleman)

- It uses public key and private key to encrypt and decrypt messages.
- RSA public key exchange is an asymmetric encryption algorithm. RSA can be used with digital signatures, key exchanges and for encryption. The RSA algorithm addresses the issue which the Diffie-Hellman algorithm is known for, by providing authentication as well as encryption. Providing RSA is used with a long key, it has proven to be a very secure algorithm.
- RSA requires a public key and private key for encrypting and decrypting data over the internet.
- RSA has been implemented in hardware and software. RSA is built into software such as Microsoft products, Apple and Novell. RSA has been implemented into hardware such as network interface cards and smart cards as well.

PGP “Pretty Good Privacy,”

- PGP stands for “Pretty Good Privacy,” and it’s most often used for sending encrypted messages between two people. PGP works by encrypting a message using a public key that’s tied to a specific user; when that user receives the message, they use a private key that’s known only to them to decrypt it.
- PGP is generally regarded as being extremely safe. The two-key system, digital signatures, and the fact that PGP is open-source and has been heavily vetted by the public all contribute to its reputation as one of the best encryption protocols.

Hashing

- Hash is a kind of process, signature, function which is responsible for translating information into a cryptic value. The concept of hash and encryption is almost same. In practical view Hash is an algorithm that takes an arbitrary block of data and returns a fixed-size bit string. Hashing is also known for its unidirectional process because it is not require rehashing or decrypting to get back data. In hashing the data which is needed to be encoded is often called the “message,” and the outcome of hash value after processing is sometimes called the message digest or simply digests.

Flowchart Example of Hash Work

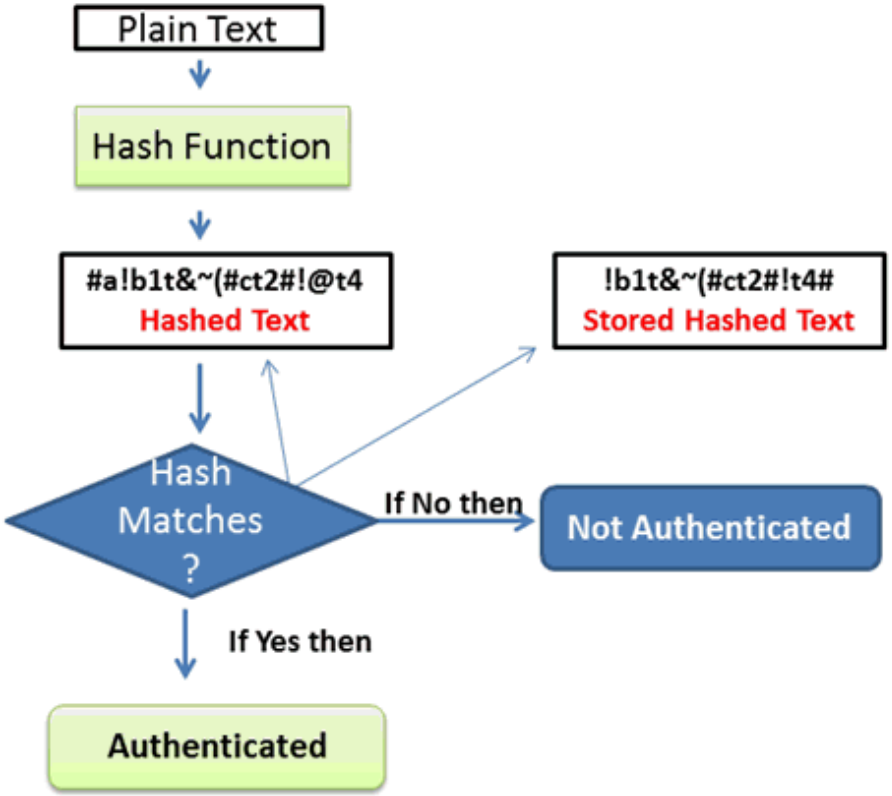


Fig : Flow Chart Example of Hash work

SSL (Secure Sockets Layer) Encryption

- SSL (Secure Sockets Layer) is a standard security protocol for establishing encrypted links between a web server and a browser in an online communication.
- The usage of SSL technology ensures that all data transmitted between the web server and browser remains encrypted.

Cont……..

SSL (Secure Sockets Layer)

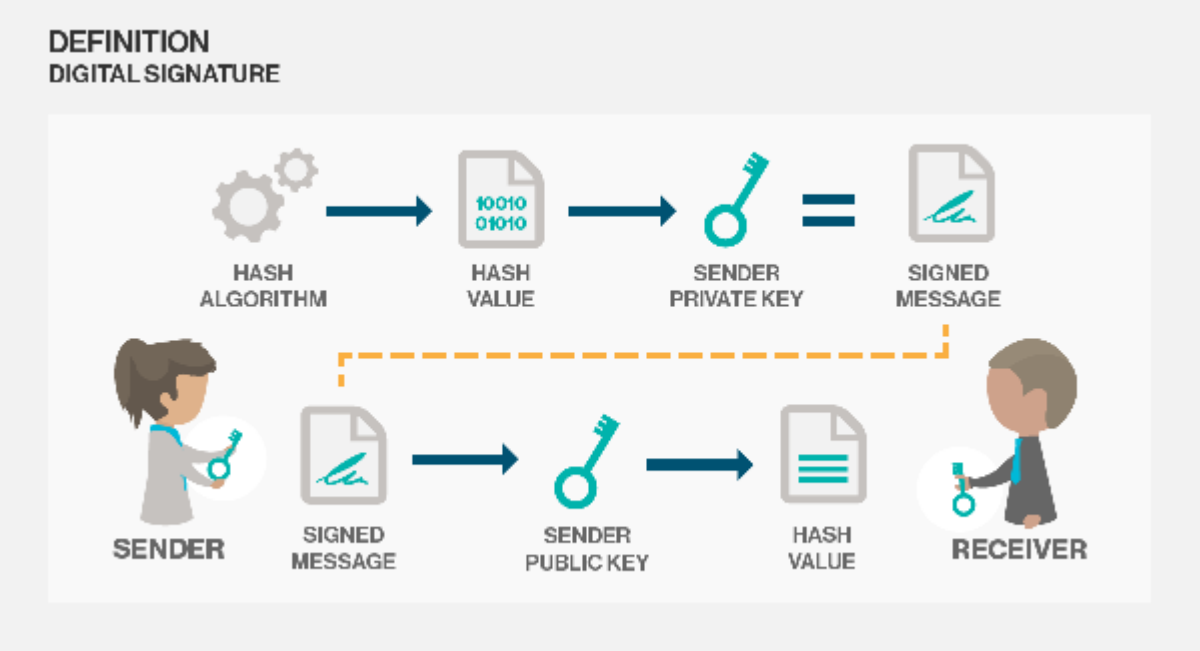
- SSL has been universally accepted on the World Wide Web for authenticated and encrypted communication between clients and servers. SSL was originally developed by Netscape in the early 90s.
- Today, everyone on the web uses SSL on a daily basis. Every major bank, as well as hundreds of thousands of sites including Google, PayPal, Facebook, and Wikipedia use SSL.

Digital Signatures

- Another feature of public-key cryptography is it allows for the creation of something called digital signatures. A digital signature can be used to authenticate data but with the added benefit of being completely unforgeable.
- A digital signature is created by a mathematical algorithm which combines your private key with data you wish to “sign”. The validity of the signature can by verified by anyone simply by checking it with your public key.

Cont…….

Digital Signatures



Thank You