IT2004 –Introduction to Data communication & Networking

Network Security

P.G.R Nayomi Gamlath
MSc(Pdn) , BSc (Rajarata)
ATI -Kurunegala

What is security ?

- The state of being free from danger or threat.
- safety

Why we need security ?

- Protect vital information while still allowing access to those who need it
- Provide authentication and access control for resources
- Guarantee availability of resources

Who is vulnerable?

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations
- **ANYONE ON THE NETWORK**

Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

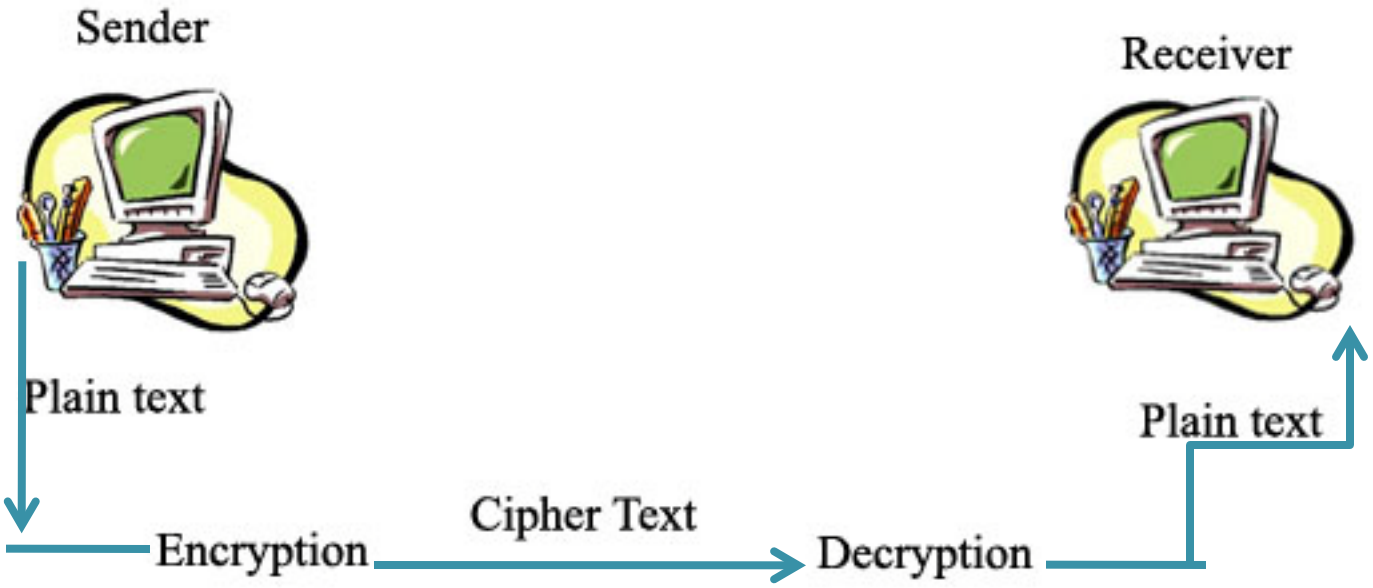
Network Security

- Security in networking is based on cryptography, the science and art of transforming messages to make them secure and immune to attack.
- Cryptography can provide several aspects of security related to the interchange of messages through networks.
- These aspects are confidentiality, integrity, authentication, and no repudiation.

Cryptography

- Network security is mostly achieved through the use of cryptography, a science based on abstract algebra.
- Cryptography, a word with Greek origins, means "secret writing.“
- However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.

Cryptography components



Plaintext and Ciphertext

- The original message, before being transformed, is called plaintext.
- After the message is transformed, it is called ciphertext.
- An encryption algorithm transforms the plaintext into ciphertext;
- A decryption algorithm transforms the ciphertext back into plaintext.
- The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.

Cipher

- We refer to encryption and decryption algorithms as ciphers.
- The term *cipher is also* used to refer to different categories of algorithms in cryptography.

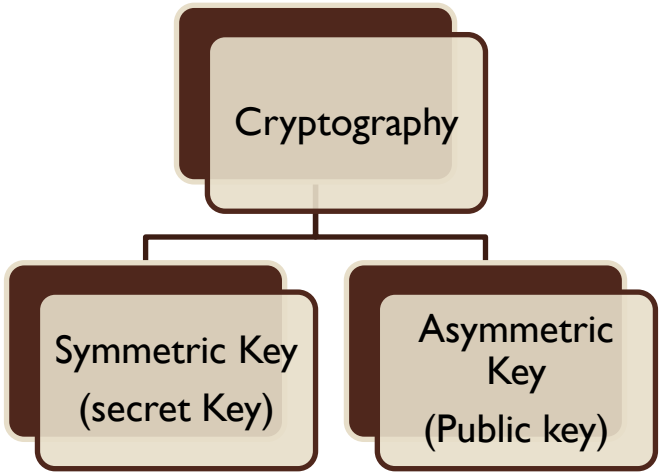
Key

- A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on.
- To encrypt a message, we need an encryption algorithm, an encryption key, and the plaintext.
- These create the ciphertext.
- To decrypt a message, we need a decryption algorithm, a decryption key, and the ciphertext.
- These reveal the original plaintext.

Cryptography algorithms

- Two categories

1. Symmetric key(also called secret-key) cryptography algorithms
2. Asymmetric Key (also called public-key) cryptography algorithms.



Symmetric Key Cryptography

- The same key is used by both parties.
- The sender uses this key and an encryption algorithm to encrypt data
- The receiver uses the same key and the corresponding decryption algorithm to decrypt the data

Asymmetric-Key Cryptography

- In asymmetric or public-key cryptography, there are two keys: a private key and a public key.
- The private key is kept by the receiver.
- The public key is announced to the public.

Example

- Imagine Alice wants to send a message to Bob.
- Alice uses the public key to encrypt the message. When the message is received by Bob, the private key is used to decrypt the message.

Asymmetric-Key Cryptography

- The public key is available to the public
- The private key is available only to an individual.

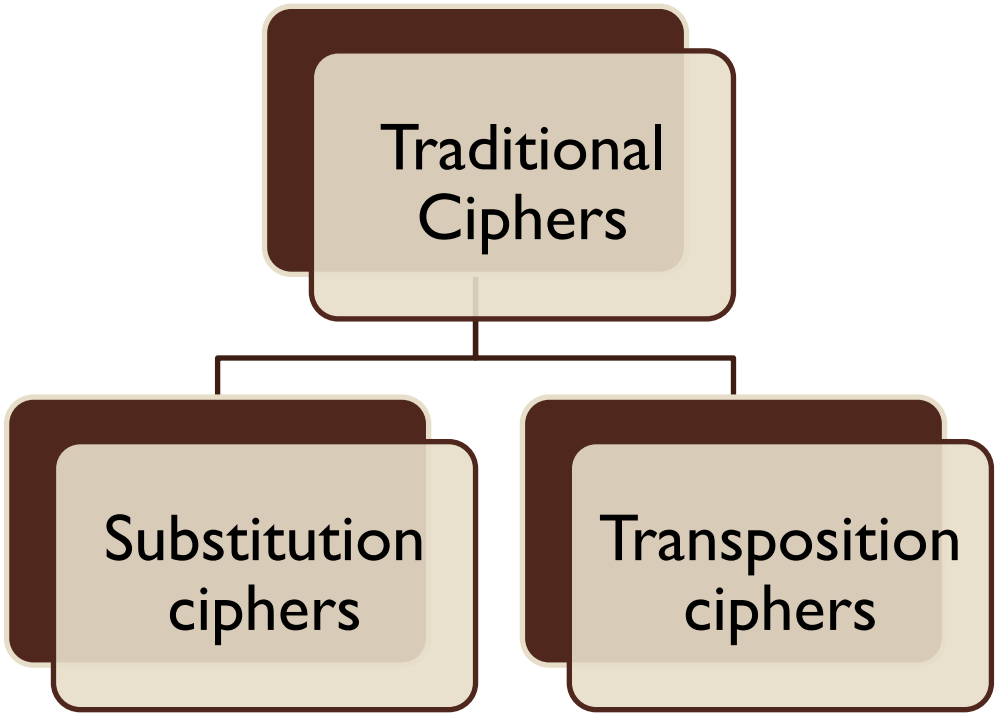
Three types of Keys in Cryptography

1. **Secret key** -is the shared key used in symmetric-key cryptography
2. **Public key -** used in asymmetric-key cryptography
3. **Private key** **-**used in asymmetric-key cryptography

Symmetric-key cryptography

- Symmetric-key cryptography started thousands of years ago when people needed to exchange secrets (for example, in a war).
- We still mainly use symmetric-key cryptography in our network security.
- Today's ciphers are much more complex.
- Traditional algorithms, which were character-oriented.
- Modern algorithms, which are bit-oriented.

Traditional Ciphers



Substitution Cipher

- A substitution cipher substitutes one symbol with another.
- If the symbols in the plaintext are alphabetic characters, we replace one character with another.
- For example, we can replace character A with D, and character T with Z.
- If the symbols are digits (0 to9), we can replace 3 with 7, and 2 with 6.

  Plaintext: HELLO

  Ciphertext: KHOOR

Substitution Cipher

- **Shift Cipher (Caesar cipher)**
- ***Example :*** Use the shift cipher with key = 15 to encrypt the message "HELLO."
- ***Solution :*** We encrypt one character at a time. Each character is shifted 15 characters down. Letter H is encrypted to W. Letter E is encrypted to T. The first L is encrypted to A. The second L is also encrypted to A. And 0 is encrypted to D. The cipher text is WTAAD.

Substitution Cipher

- **Shift Cipher (Caesar cipher)**
- **Example :** Use the shift cipher with key =15 to decrypt the message "WTAAD."
- **Solution** :We decrypt one character at a time. Each character is shifted 15 characters up. Letter W is decrypted to H. Letter T is decrypted to E. The first A is decrypted to L. The second A is decrypted to L. And, finally, D is decrypted to O. The plaintext is HELLO.

Transposition Ciphers

- In a transposition cipher, there is no substitution of characters; instead, their locations change.
- A character in the first position of the plaintext may appear in the tenth position of the ciphertext.
- A character in the eighth position may appear in the first position.
- In other words, a transposition cipher reorders the symbols in a block of symbols.
  - Plaintext: 2 4 1 3
  - Ciphertext: 12 3 4

Firewall

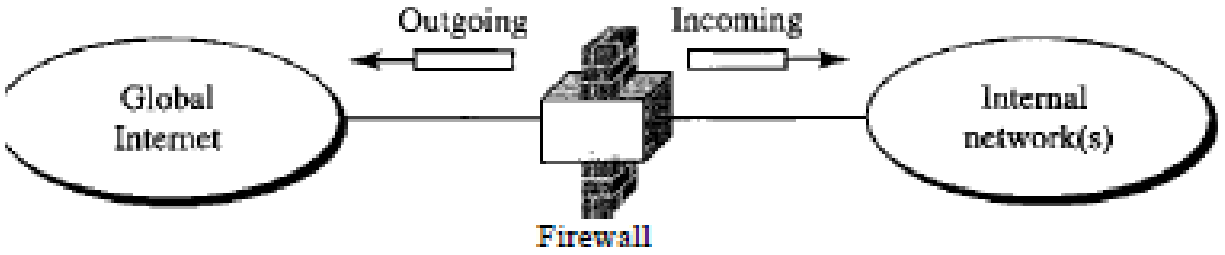
- Many network applications and protocols have security problems that are fixed over time
  - Difficult for users to keep up with changes and keep host secure
  - Solution
    - Administrators limit access to end hosts by using a firewall
    - Firewall is kept up-to-date by administrators

Firewall

- A firewall is like a castle with a drawbridge
  - Only one point of access into the network
  - This can be good or bad
- Can be hardware or software
  - Ex. Some routers come with firewall functionality
  - Windows XP, viata ,7 have built in firewalls

Firewall

- A firewall as a hardware device (usually a router or a computer) is installed between the internal network of an organization and the rest of the Internet.
- It is designed to forward some packets and filter (not forward) others.



Firewall

- A firewall may filter all incoming packets destined for a specific host or a specific server such as HTTP.
- A firewall can be used to deny access to a specific host or a specific service in the organization.

Reference

- Data communication & Networking by Behrouz A. Forouzan