Wollo University

Kombolcha Institute of Technology

Department of Information Technology

Data Communication and Computer Networks(SEng2092)

Chapter 08:

DATA SECURITY AND INTEGRITY

8.1 Fundamentals Of Secure Networks; Cryptography

Security: allowing people to see what you want them to see and preventing them from seeing what you don't want them to see.

Cryptography comes from the Greek words for "*secret writing*".

Professionals make a distinction between ciphers and codes.

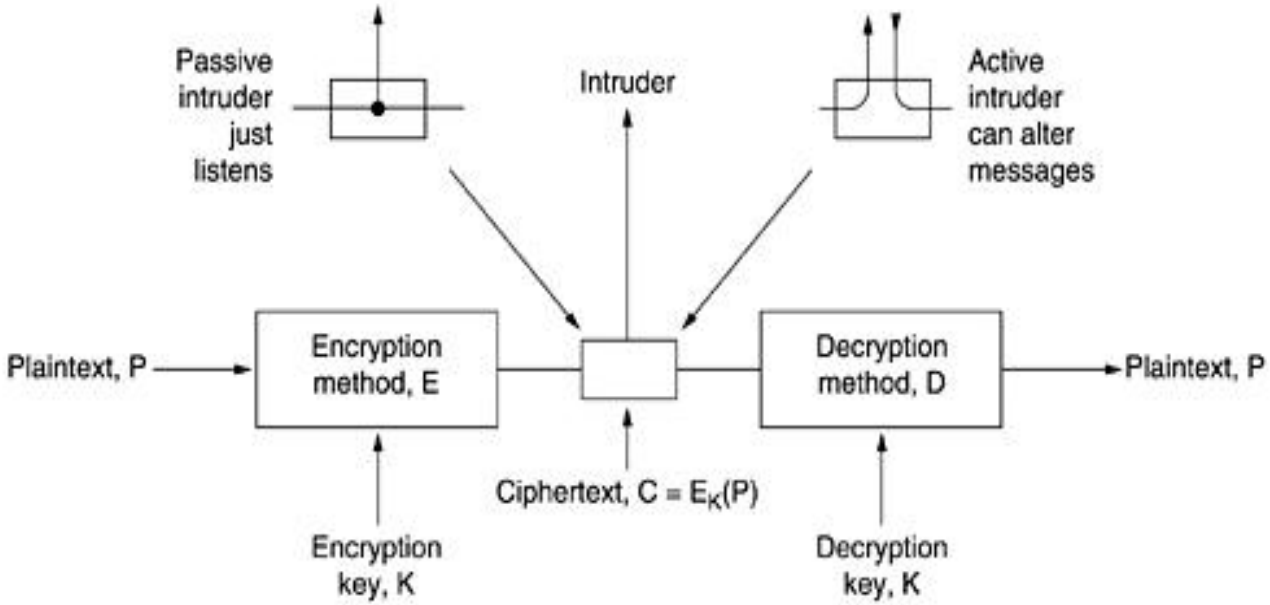
A cipher is a character-for-character or bit-for-bit transformation, without regard to the linguistic structure of the message. In contrast,

a code replaces one word with another word or symbol. Codes are not used any more, although they have a glorious history.

- Historically, four groups of people have used and contributed to the art of cryptography: **the military, the diplomatic corps, diarists, and lovers**.
- The messages to be encrypted, known as the plaintext, are transformed by a function that is parameterized by a key.
- The output of the encryption process, known as the ciphertext, is then transmitted, often by messenger or radio.
- We assume that the enemy, or intruder, hears and accurately copies down the complete cipher text. However, unlike the intended recipient, he does not know what the decryption key is and so cannot decrypt the cipher text easily.

- Sometimes the intruder can not only listen to the communication channel (passive intruder) but can also record messages and play them back later, inject his own messages, or modify legitimate messages before they get to the receiver (active intruder).
- The art of breaking ciphers, called cryptanalysis, and the art devising them (cryptography) is collectively known as cryptology.
- It will often be useful to have a notation for relating plaintext, ciphertext, and keys.
- We will use $C = E_K(P)$ to mean that the encryption of the plaintext P using key K gives the ciphertext C. Similarly, $P = D_K(C)$ represents the decryption of C to get the plaintext again. It then follows that $D_K(E_K(P))=P$.

Figure 8.1: The encryption model (for a symmetric-key cipher)



A fundamental rule of cryptography is that one must assume that the cryptanalyst knows the methods used for encryption and decryption. In other words, the cryptanalyst knows how the encryption method, E, and decryption, D,of Figure 8.1 work in detail.

What is Cipher ?

- ✓ In the network security concept Cipher means hiding or coding of the data when the client sent it.
- ✓ Or it means the data on the network.

1. Substitution Technique is one in which the letters/numbers/symbol of the plain text are replaced by other letters/numbers/symbols.

Eg. A➔D, T➔Z, Or 2➔5, 3➔6.

2. Transposition technique the position of the letter/numbers/symbols in plaintext is changed with one another.

PT➔

CT➔

H	E	L	L	O	C	L	A	S	S
O	L	L	E	H	S	S	A	L	C

- ✓ Plain text: HELLO CLASS
- ✓ Cipher text: OLLEHSSALC

3. Rail fence Cipher

PT➔ HELLO CLASS!

CP➔HOSELCASLL!

H	-	-	-	O	-	-	-	S	-	-
-	E		L		C		A		S	
-	-	L				L				!

4. ROUT CIPHER

PT➔ I WILL COME TOMORROWX

CT➔CLLIWIOORROWXMOTEM

I	O	O
W	M	R
I	E	R
L	T	O
L	O	W
C	M	X

8.2 Encryption and Privacy Policy

- privacy policy:- is a statement or a legal document (in privacy law) that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data.
- *Encryption :-*It is the process of scrambling (compress, secure) the contents of a file or message to make it unintelligible to anyone not in possession of the "key" required to unscramble the file or message.

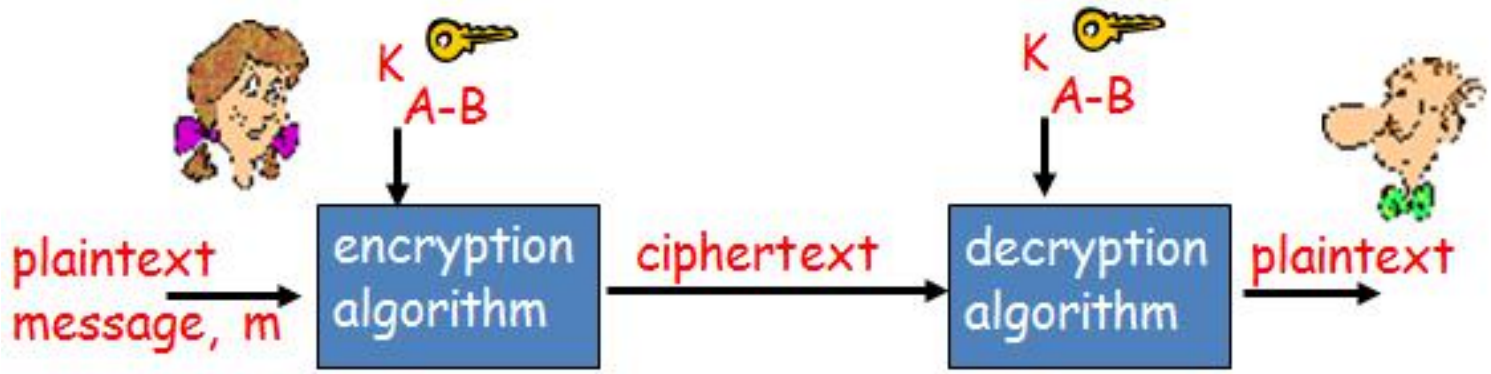
There are two types of encryption:

A. symmetric (private/secret) key and
B. Asymmetric (public) key.

Encryption and Privacy Policy

A. Symmetric Key Encryption

- ✓ When most people think of encryption it is symmetric key cryptosystems that they think of.
- ✓ Symmetric key, also referred to as private key or secret key, is based on a single key and
- ✓ algorithm being shared between the parties who are exchanging encrypted information.
- ✓ The same key both encrypts and decrypts messages.



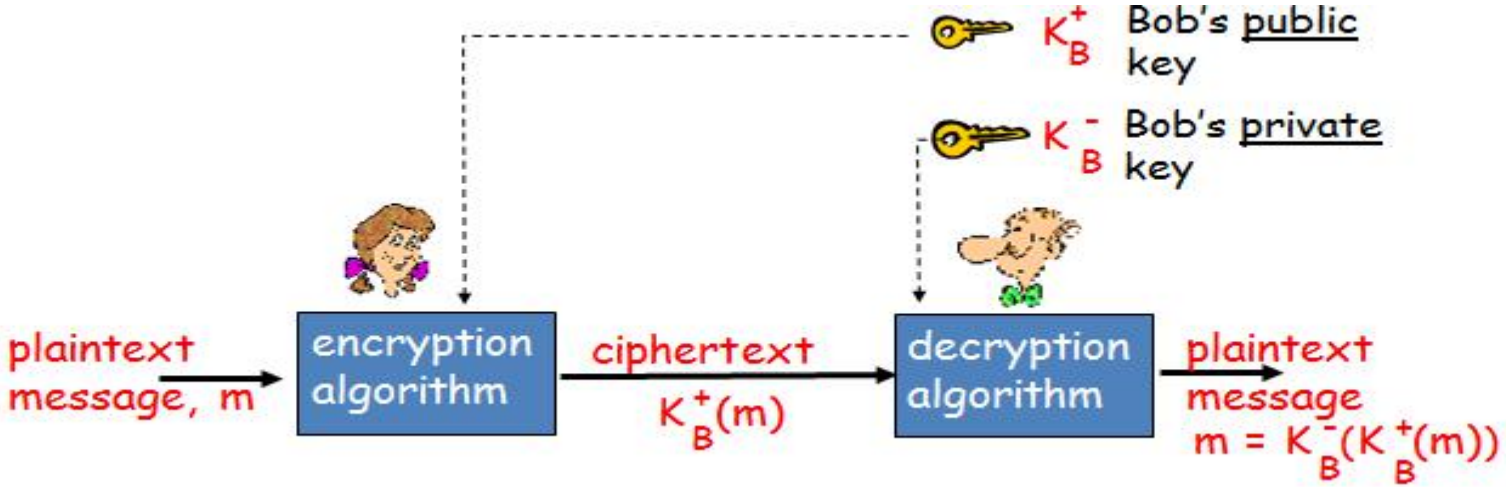
Encryption and Privacy Policy…

B. Public Key Encryption

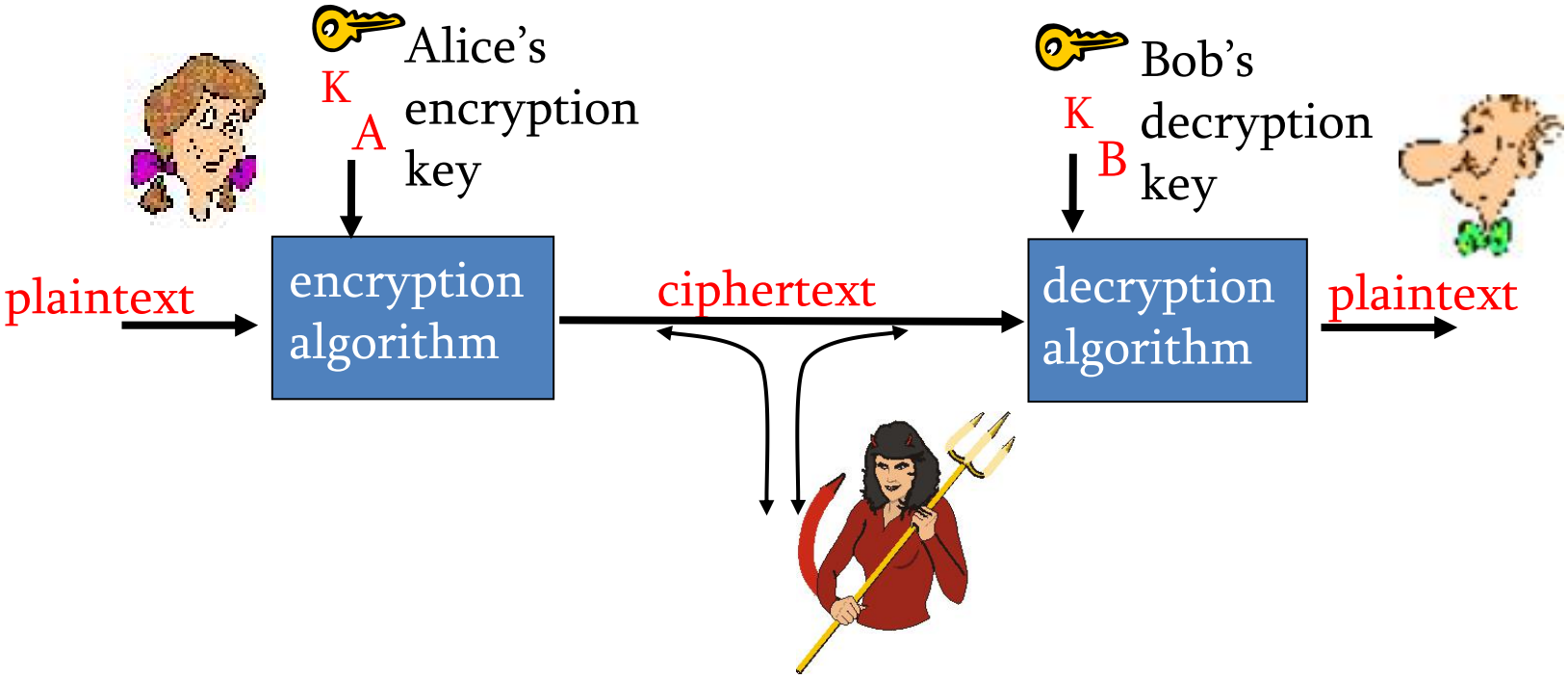
requires sender, receiver know shared secret(public) key

public key Encryption

- radically different approach
- sender, receiver do *not* share secret key
- *public* encryption key known to *all*
- *private* decryption key known only to receiver



The language of cryptography



symmetric key crypto: sender, receiver keys *identical*

public-key crypto: encryption key *public*, decryption key *secret* (private)

8.3 Authentication Protocol

- Authentication is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter. Verifying the identity of a remote process in the face of a malicious, active intruder is surprisingly difficult and requires complex protocols based on cryptography. In this section, we will study some of the many authentication protocols that are used in secure computer networks.
- As an aside, some people confuse authorization with authentication.
- **Authentication** deals with the question of whether you are actually communicating with a specific process.
- **Authorization** is concerned with what that process is permitted to do.

Authentication Protocol…

- For example, a client process contacts a file server and says: I am Scott's process and I want to delete the file cookbook.old. From the file server's point of view, two questions must be answered:
- Is this actually Scott's process (authentication)?
- Is Scott allowed to delete cookbook.old (authorization)?
- Only after both of these questions have been unambiguously answered in the affirmative can the requested action take place. The former question is really the key one. Once the file server knows to whom it is talking, checking authorization is just a matter of looking up entries in local tables or databases. For this reason, we will concentrate on authentication in this section.

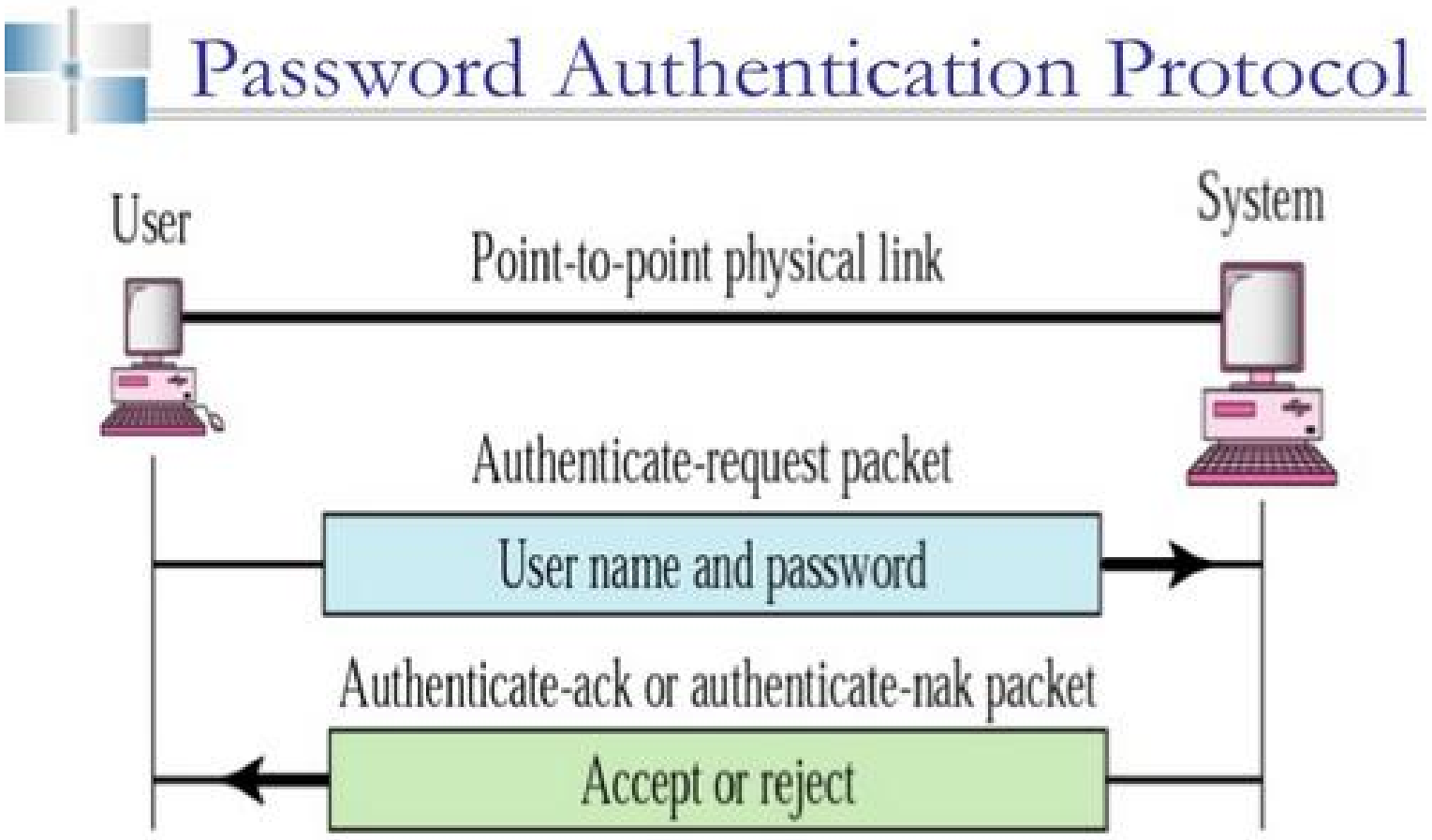
Authentication Protocol…

- The general model that all authentication protocols use is this. Alice starts out by sending a message either to Bob or to a trusted KDC (Key Distribution Center), which is expected to be honest. Several other message exchanges follow in various directions. As these messages are being sent Trudy may intercept, modify, or replay them in order to trick Alice and Bob or just to gum up the works.
- Nevertheless, when the protocol has been completed, Alice is sure she is talking to Bob and Bob is sure he is talking to Alice. Furthermore, in most of the protocols, the two of them will also have established a secret session key for use in the upcoming conversation.

Authentication Protocol…

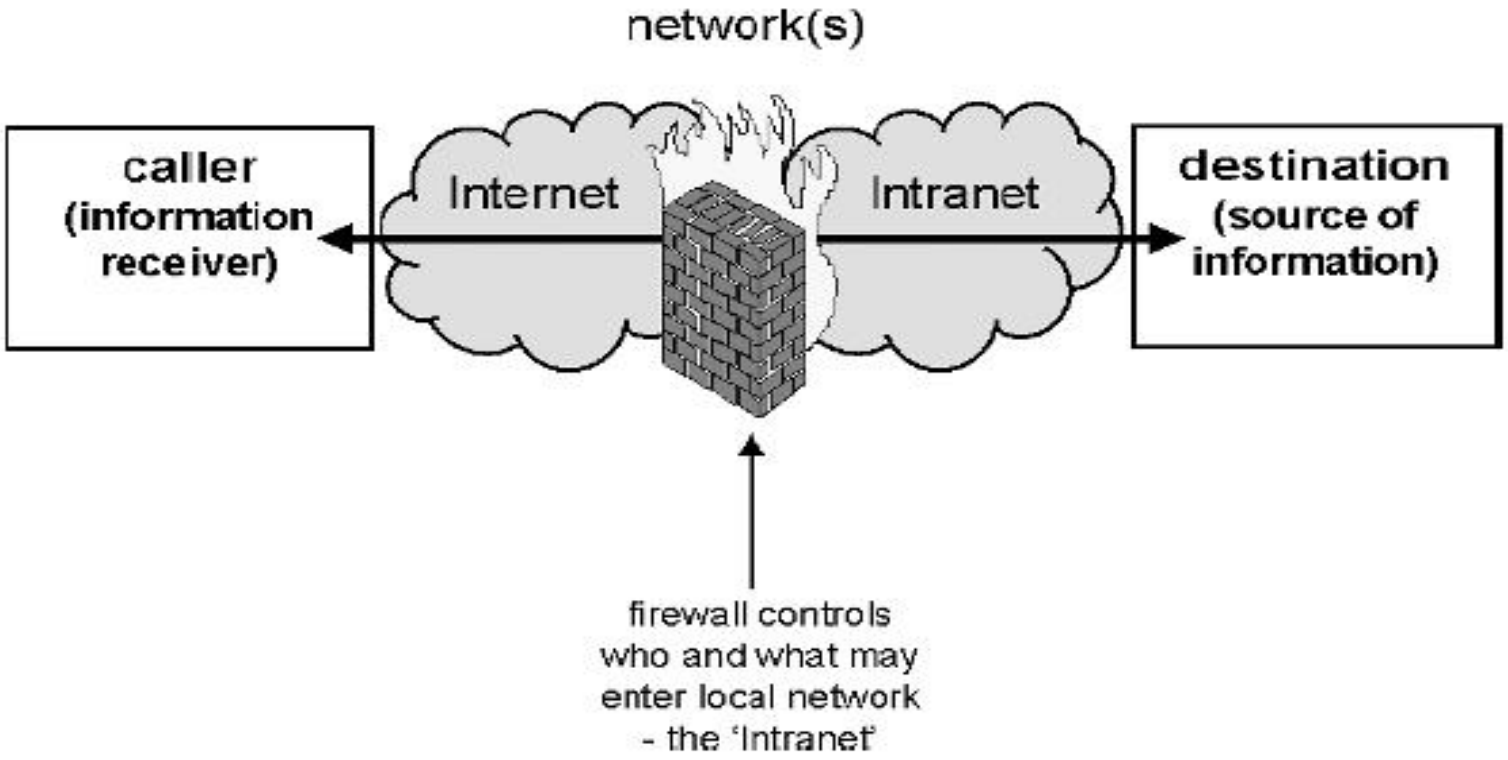
- In practice, for performance reasons, all data traffic is encrypted using symmetric-key cryptography (typically AES or triple DES), although public-key cryptography is widely used for the authentication protocols themselves and for establishing the session key.
- The point of using a new, randomly-chosen session key for each new connection is to minimize the amount of traffic that gets sent with the users' secret keys or public keys, to reduce the amount of ciphertext an intruder can obtain, and to minimize the damage done if a process crashes and its core dump falls into the wrong hands. Hopefully, the only key present then will be the session key. All the permanent keys should have been carefully zeroed out after the session was established.

Authentication Protocol…



8.4 Firewalls

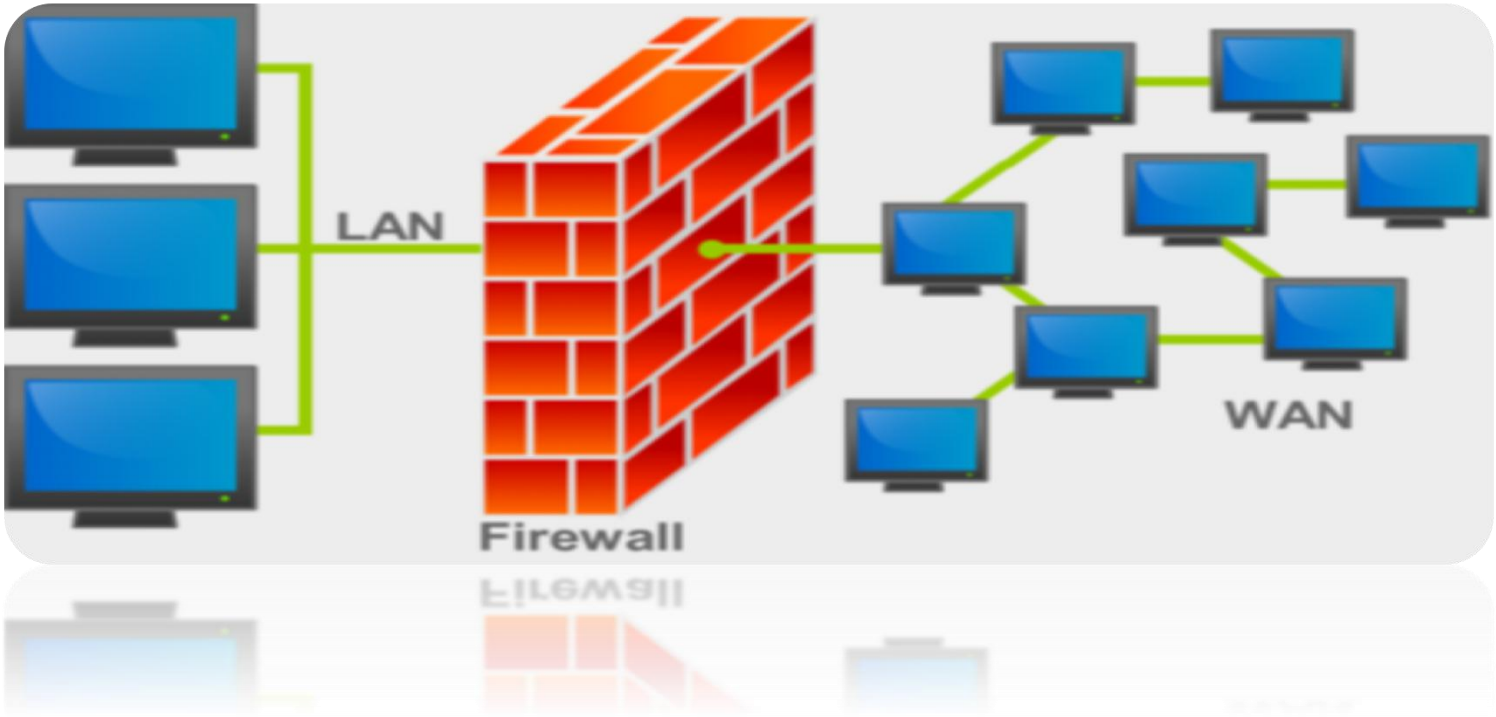
- A firewall is a device used to protect a private (typically company-internal) intranet from intrusions by unauthorised third-parties attempting to gain access from the public Internet,



Firewalls…

- Firewalls: a means of protecting company 'Intranets' from intrusion by users of the public Internet.
- The firewall may comprise of one or a number of different devices, which together are intended to control:
  - which external users (i.e., Internet users) may access the intranet;
  - which servers these external users may access;
  - which information may be exported from these servers; and
  - what type of information may be sent into the network.

Firewalls…



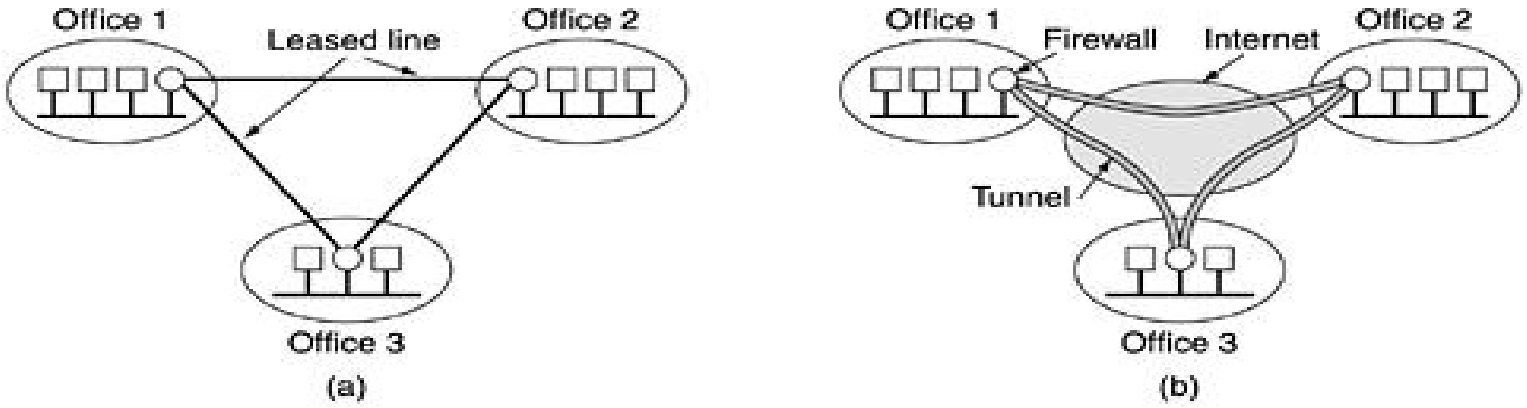
- Firewalls typically comprise routers, application *proxies* and *content filters* (including *virus scanners*).
- Firewall routers are used to check source and destination IP addresses and to allow communication only between allowed combinations of source and destination.
- *Application proxies* protect the 'real' application servers by checking the communication between the external user and the server. Only 'acceptable' requests are actually relayed to and from the 'real' application server.
- Content filters are used to check the nature of data sent into the network. The objective is to prevent intrusion by *viruses* or other harmful data or application programs.

Firewall function

- **First generation: packet filters**
  - The first type of firewall was the packet filter which looks at network addresses and ports of the packet and determines if that packet should be allowed or blocked
- **Second generation: "tasteful" filters**
  - Second-generation firewalls perform the work of their first-generation predecessors but operate up to layer 4 (transport layer) of the OSI model.

8.5 Virtual Private Network(VPN)

- Many companies have offices and plants scattered over many cities, sometimes over multiple countries. In the olden days, before public data networks, it was common for such companies to lease lines from the telephone company between some or all pairs of locations. Some companies still do this.
- A network built up from company computers and leased telephone lines is called a private network. An example private network connecting three locations is shown in the figure depicted below.



VPN…

- Private networks work fine and are very secure. If the only lines available are the leased lines, no traffic can leak out of company locations and intruders have to physically wiretap the lines to break in, which is not easy to do. The problem with private networks is that leasing a single T1 line costs thousands of dollars a month and T3 lines are many times more expensive. When public data networks and later the Internet appeared, many companies wanted to move their data (and possibly voice) traffic to the public network, but without giving up the security of the private network.

VPN…

This demand soon led to the invention of VPNs (Virtual Private Networks), which are overlay networks on top of public networks but with most of the properties of private networks. They are called "virtual" because they are merely an illusion, just as virtual circuits are not real circuits and virtual memory is not real memory.

Although VPNs can be implemented on top of ATM (or frame relay), an increasingly popular approach is to build VPNs directly over the Internet. A common design is to equip each office with a firewall and create tunnels through the Internet between all pairs of offices, as illustrated in figure depicted above(b).

- VPN technology is also used by individual Internet users to secure their wireless transactions, to circumvent geo-restrictions and censorship, and to connect to proxy servers for the purpose of protecting personal identity and location.

8.6 Transport Layer Security

- **Transport Layer Security** (**TLS**) is a cryptographic protocols designed to provide communications security over a computer network.
- applicable to secure web browsing, email, Internet faxing, instant messaging, and voice-over-IP (VoIP). And
- Major web sites (including Google, YouTube, Facebook and many others) use TLS to secure all communications between their servers and web browsers.
- The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating computer applications, (a client (e.g. a web browser) and a server (e.g. wikipedia.org))

Transport Layer Security…

- The connection is private because symmetric cryptography is used to encrypt the data transmitted.
- The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated at the start of the session (see Handshake Protocol).
- The server and client negotiate the details of which encryption algorithm and cryptographic keys to use before the first byte of data is transmitted.
- The identity of the communicating parties can be authenticated using public key cryptography. This authentication can be made optional, but is generally required for at least one of the parties (typically the server).

Transport Layer Security…

- It provides for confidentiality and data integrity over a connection between two end points
- TLS operates on a reliable transport, such as TCP, and is itself layered into
  i. TLS Record Protocol
  ii. TLS Handshake Protocol

Transport Layer Security…

TLS Record Protocol

- ✓ TLS Record Protocol layers on top of a reliable connection-oriented transport, such as TCP.
- ✓ TLS Record Protocol
  - provides data confidentiality using symmetric key cryptography
  - provides data integrity using a keyed message authentication checksum (MAC)
- ✓ The keys are generated uniquely for each session based on the security parameters agreed during the TLS handshake

Transport Layer Security…

- Basic operation of the TLS Record Protocol
  1. Read messages for transmit
  2. Fragment messages into manageable chunks of data
  3. Compress the data, if compression is required and enabled
  4. Calculate a MAC
  5. Encrypt the data
  6. Transmit the resulting data to the peer

Transport Layer Security…

- At the opposite end of the TLS connection, the basic operation of the sender is replicated, but in the reverse order
  1. Read received data from the peer
  2. Decrypt the data
  3. Verify the MAC
  4. Decompress the data, if compression is required and enabled
  5. Reassemble the message fragments
  6. Deliver the message to upper protocol layers

Transport Layer Security…

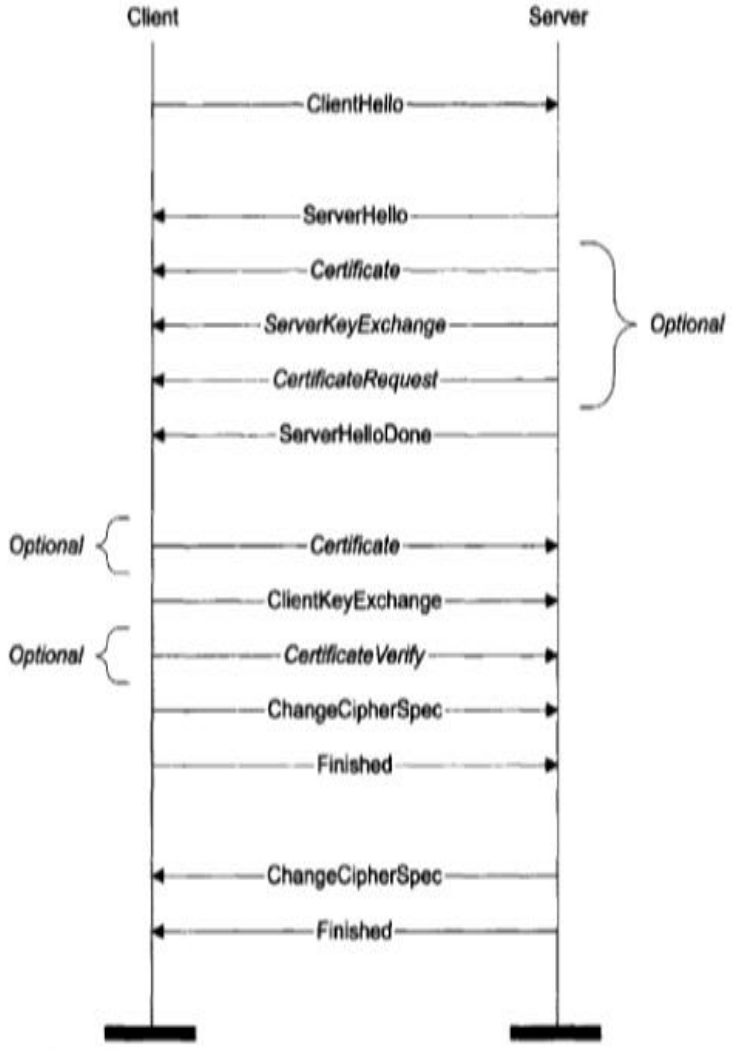
- TLS Handshake Protocol is layered on top of the TLS Record Protocol
- TLS Handshake Protocol is used to
  - ✓ Authenticate the client and the server
  - ✓ Exchange cryptographic keys
  - ✓ Negotiate the used encryption and data integrity algorithms before the applications start to communicate with each other

TLS Handshake Protocol

- The Figure illustrates the actual handshake message flow

[Step1]

- the client and server exchange Hello messages
- the client sends a ClientHello message, which is followed by the server sending a ServerHello message
- these two messages establish the TLS protocol version, the compression mechanism used, the cipher suite used, and possibly the TLS session ID
- additionally, both a random client nonce and a random server nonce are exchanged that are used in the handshake later on



TLS Handshake Protocol

[Step2]

- ✓the server may send any messages associated with the ServerHello
- ✓depending on the selected cipher suite, it will send its certificate for authentication
- ✓the server may also send a key exchange message and a certificate request message to the client, depending on the selected cipher suite
- ✓to mark the end of the ServerHello and the Hello message exchange, the server sends a ServerHelloDone message

TLS Handshake Protocol

[Step3]

- ✓next, if requested, the client will send its certificate to the server
- ✓in any case, the client will then send a key exchange message that sets the pre-master secret between the client and the server
- ✓optionally, the client may also send a Certificate Verify message to explicitly verify the certificate that the server requested

TLS Handshake Protocol

[Step4]

- ✓ then, both the client and the server send the ChangeCipherSpec messages and enable the newly negotiated cipher spec
- ✓ the first message passed in each direction using the new algorithms, keys and secrets is the Finished message, which includes a digest of all the handshake messages
- ✓ each end inspects the Finished message to verify that the handshake was not tampered with

Digest of all the handshake messages

- ✓ means the results of applying a one-way hash function to the handshake messages

Summary of TLS

- TLS protocol provides transport layer security for Internet applications and confidentiality using symmetric key cryptography and data integrity using a keyed MAC
- It also includes functionality for client and server authentication using public key cryptography

CHAPTER END

???