## Unit 4: Network Security

**Security:**

Security, in information technology (IT), is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services.

**Computer Security:** It is a process and the collection of measures and controls that ensures the Confidentiality, Integrity and Availability (CIA) of the assets in computer systems. Computer Security protects you from both software and hardware parts of a computer system from getting compromised and being exploited.

**Information Security:** Information security is primarily concerned with making sure that data in any form is kept secure in terms of preserving its confidentiality, integrity and availability.

Information is a significant asset that can be stored in different ways such as digitally stored, printed, written on papers or in human memory. It can be communicated through different channels such as spoken languages, gestures or using digital channels such as email, SMS, social media, video, audio etc.

Information security differs from cybersecurity such that information security aims to keep data in any form secure, whereas cybersecurity protects only digital data. Cybersecurity is the subset of information security.

**Network Security:** It is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Network security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure.

An effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.

Network security, a subset of cybersecurity, aims to protect any data that is being sent through devices in your network to ensure that the information is not changed or intercepted.

**Security Threats:** Security threat is possible danger that might exploit vulnerabilities in a computer system to breach security and thus cause possible harm. Vulnerability is weakness or flaw in a computer system that can be exploited by a threat. Simply, we can say that threat is the intersection of actor, motivation and vulnerability.

A threat is something that may or may not happen, but has the potential to cause serious damage. A threat can be either intentional or accidental. Intentional threats are normally due to intelligent persons like crackers or hackers or criminal organizations. On the other hand, accidental threats are due to malfunctioning of computers or due to natural disasters or due to mistakes done by computer users. There are four types of security threats:

**1.Interception:** Interception refers to the situation that an unauthorized party has gained access to a service or data. A typical example of interception is where communication between two parties has been overheard by someone else.

**2.Interruption:** Interruption refers to the situation, in which services or data become unavailable, unusable, destroyed, and so on. Making the service inaccessible to others parties can be considered as interruption.

**3.Modification:** Modification involves unauthorized changing of data or tampering with a service so that it no longer adheres to its original specification. Examples of modification include intercepting and subsequently changing transmitted data.

**4.Fabrication:** Fabrication refers to the situation in which additional data or activities are generated that would normally not exist. For example, an intruder may attempt to add an entry into a password file or database.

**Security attacks:** An attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. Intruders first of all analyze our environment and collect information in order to exploit vulnerabilities and then perform the desired type of attack in our computer system. Our networks and data are vulnerable to any of the following types of attacks if you do not have a security plan in place.

**1.Passive Attacks:** An attack that attempts to learn or make use of information from the system but does not affect system resources is called passive attacks. It includes traffic analysis, monitoring of unprotected communication, decrypting weakly encrypted traffic, and capturing authentication information such as password. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

**2. Active Attacks:** An attack that attempts to alter system resources or affect their operation is called active attacks. This can be done through stealth, virus, worms, or Trojan horses. Active attacks result in the disclosure or dissemination of data files, Denial of Services or modification of data.

**Security Principles/Security Services (CIA Triad):**

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization.


**Confidentiality**: Preserving authorized restrictions on information access and disclosure. This term covers two related concepts:

Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

**Integrity:** Guarding against improper information modification or destruction. This term covers two related concepts:

Data integrity: Assures that information (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner.

System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

**Availability:** Assures that systems work promptly and service is not denied to authorized users.

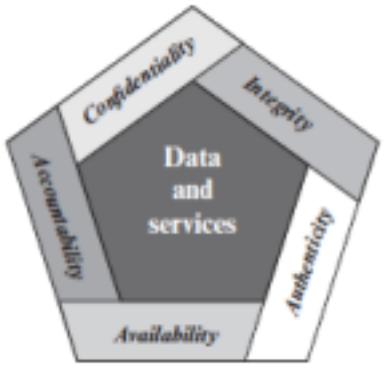



Figure 1.1 Essential Network and Computer Security Requirements

**Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

**Accountability:** It means that every individual who works with an information system should have specific responsibilities for information assurance.

**Access Control:** The prevention of unauthorized use of a resource.

**Nonrepudiation:** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

**E-Commerce Security Concerns:**

Security concerns in electronic commerce can be divided into two broad categories: Client Server Security and Data & Message Security.

Client Server Security:

- It uses various authentication and authorization methods to make sure that only valid users and programs have access to information resources such as databases.
- Access control mechanisms are enabled to ensure that only authorized users are allowed to use

resources.

Data and Transaction Security:

- It ensures privacy and confidentiality in electronic message and data packets. • It includes authentication of remote users in network transactions for online payments. • Different preventive measures like encryption approaches are used to achieve data and transaction security.

**Data and Message Security:**

Since the invention of the World Wide Web' (WWW) in 1989, Internet-based electronic commerce has been transformed from a mere idea into reality. Consumers search for best offers, order goods, and pay them electronically. Most financial institutions have some sort of online presence, allowing their customers to access and manage their accounts, make financial transactions, trade stocks, and so forth. Electronic mails are exchanged within and between enterprises, and often already replace fax copies. Soon there is arguably no enterprise left that has no Internet presence. Thus, doing some electronic business on the Internet is already an easy task.

At the same time several reasons contribute to this insecurity: Eavesdropping and acting under false identity is simple. Stealing data is undetectable in most cases. Popular PC operating systems offer little or no security against viruses or other malicious software, which means that users cannot even trust the information displayed on their own screens. Therefore, if the security and privacy problems are addressed, e-shoppers will be converted into e-buyers, and ecommerce will be pushed a big step forward. Ecommerce transaction security issues can be divided into two types: Data and Message security.

**Data Security:**

It is of principal importance at a time when people are considering banking and other Financial transactions by PCs. A major threat to data security is unauthorized network monitoring, also called packet
sniffing. It involves capturing, decoding, inspecting and interpreting the information inside a network packet. The purpose is to steal information, usually user IDs, passwords, network details, credit card numbers, etc. Sniffing is generally referred to as a passive type of attack, wherein the attackers can be silent/invisible on the network. This makes it difficult to detect, and hence it is a serious type of attack.

**Message Security:**

Secure transmission is concerned with the techniques and practices that will guarantee protection from eavesdropping and intentional message modification. Threats to message security fall into three categories: Confidentiality, Integrity and Authentication.

***Message Confidentiality:*** Confidentiality is maintaining the secrecy or privacy of a message. Cryptography can be the better choice for maintaining the privacy of information, which traditionally is used to protect the secret messages. Similarly, privacy of resources i.e., resource hiding can be maintained by using proper firewalls. Confidentiality is important for users involving sensitive data such as credit card numbers.

***Message Integrity:*** Integrity ensures the correctness as well as trustworthiness of data or resources. For example, if we say that we have preserved the integrity of an item, we may mean that the item is:

precise, accurate, unmodified, modified only in acceptable ways, modified only by authorized people, modified only by authorized processes, consistent, meaningful and usable. Integrity mechanisms fall into two classes, prevention mechanisms and detection mechanisms. Prevention mechanisms are responsible to maintain the integrity of data by blocking any unauthorized attempts to change the data or any attempts to change data in unauthorized ways. While in detection mechanisms, they simply analyze the data's integrity and are no longer trustworthy.

***Message Authentication**:* For e-commerce, it is important that clients authenticate themselves to servers that servers authenticate to each other. Authentication is a mechanism whereby the receiver of a transaction or message can be confident of the identity of the sender and/or integrity of the message. Authentication in e-commerce basically requires the user to prove his or her identity for each requested service.

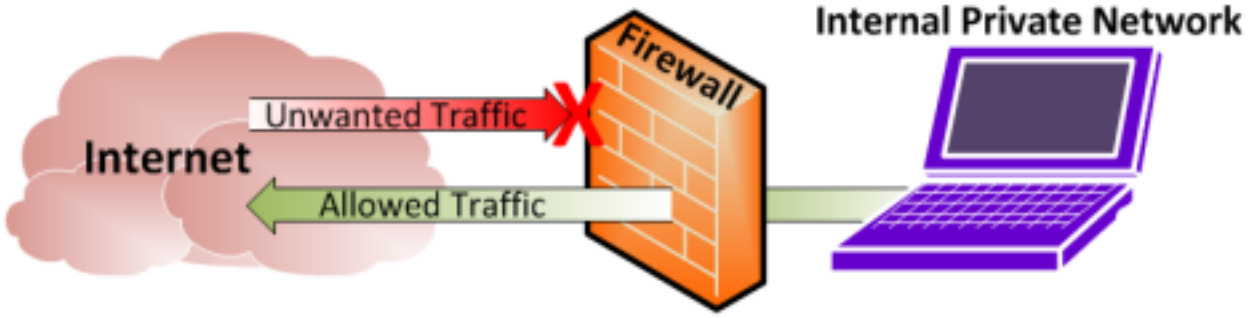
**Reasons for Data and Message Security:**

- Ensure Business Continuity, prevent loss of revenue
- Avoid Data Breaches and Misuse
- Prevent Unauthorized Access and Manipulation
- Protect the Assets
- Protect Customer's Privacy
- Maintaining and Improving Brand Value
- Competitive Advantage over other Businesses

**Firewall:**

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It typically establishes a barrier between a trusted internal network and an untrusted external network, such as the Internet.

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. All messages entering or leaving the private network pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. Hardware firewalls can be purchased as a stand-alone product but are also typically found in routers, and should be considered as an important part of system and network set-up.




Software firewalls are installed on your computer (like any software) and we can customize it; allowing us some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access to your computer. There are several types of firewall techniques:

- Packet Filtering Firewalls
- Stateful Inspection Firewall
- Circuit-Level Gateways
- Application Gateways

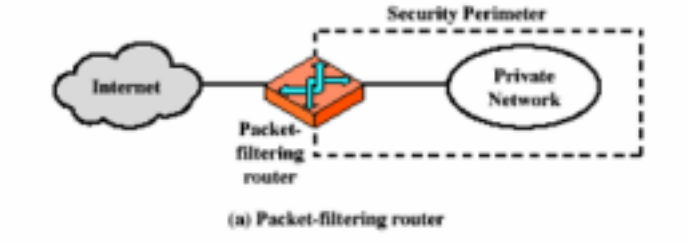
**Packet filtering firewall:**

- A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.
- The firewall is typically configured to filter packets going in both directions (from and to the internal network).
- Filtering rules are based on information contained in a network packet.

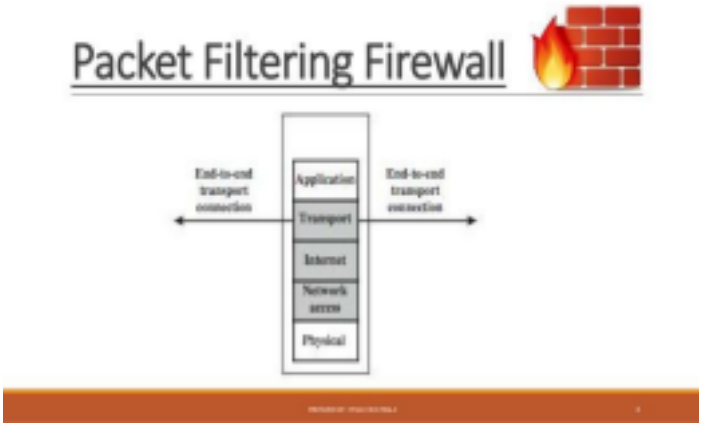
Two default policies are possible:

1. **Default = discard:** That which is not expressly permitted is prohibited.
2. **Default = forward:** That which is not expressly prohibited is permitted.

Advantage of a packet filtering firewall is its simplicity. Also, packet filters typically are transparent to users and are very fast.

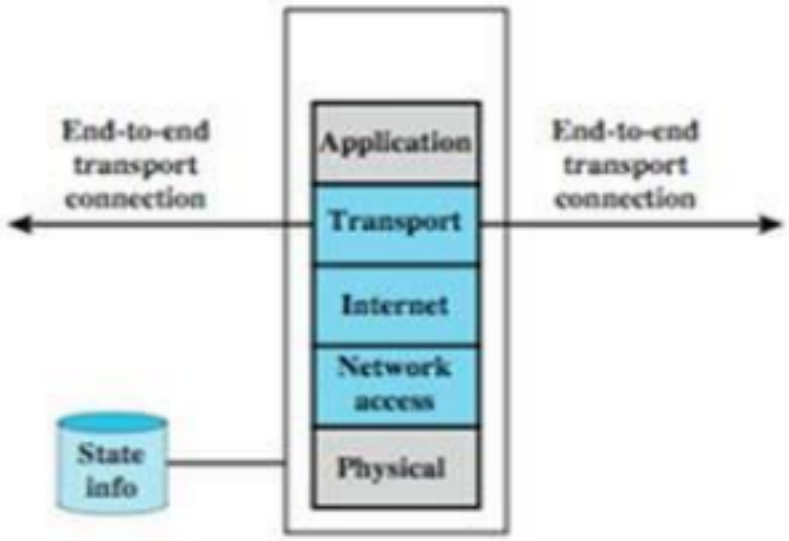


(a) Packet-filtering router




**State-full Inspection Firewall:**

- State-full packet filtering is a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall. • It is also known as dynamic packet filtering and Stateful inspection filtering. • Only packets matching a known active connection are allowed to pass the firewall. • It is a security feature often included in business networks.



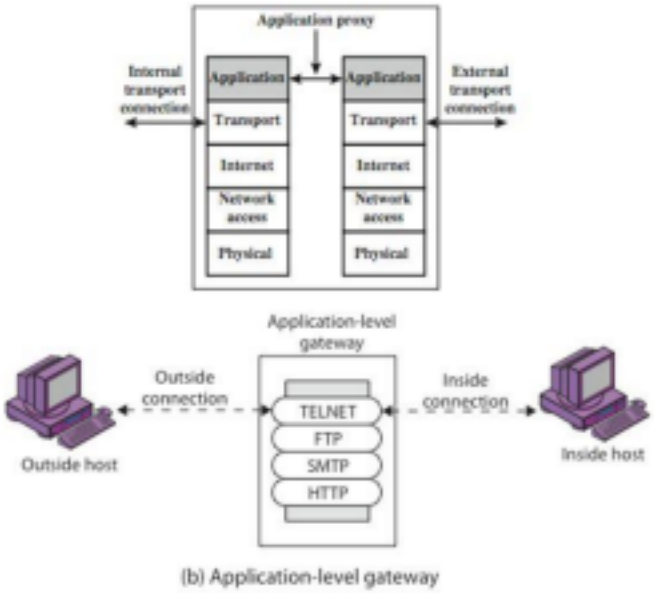

(c) Stateful inspection firewall

- A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections.
- There is an entry for each currently established connection.
- The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.
- By recording session information such as IP addresses and port numbers, a dynamic packet filter can implement a much tighter security posture than a static packet filter can.

**Application-Level Gateway:**

- An application-level gateway, also called an application proxy**,** acts as a relay of application-level traffic.
- The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.
- When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.

# Firewalls - Application Level Gateway (or Proxy)



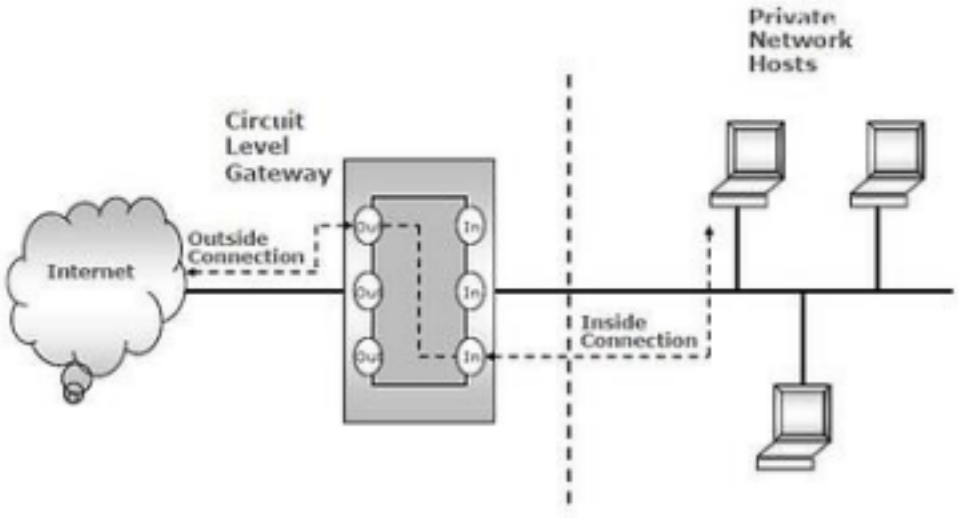

(b) Application-level gateway



- If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall.
- Application proxy filters incoming node traffic to certain specifications which mean that only transmitted network application data is filtered.
- Application-level gateways tend to be more secure than packet filters.
- In addition, it is easy to log and audit all incoming traffic at the application level.
- Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application-level gateway need only examine a few allowable applications.

**Circuit Level Gateway:**

- A fourth type of firewall is the circuit-level gateway or circuit-level proxy**.**
- The circuit level gateway firewalls work at the transport and session layer of the OSI model. They monitor TCP handshaking between the packets to determine if a requested session is legitimate.
- As with an application gateway, a circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host.




- Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents.
- The security function consists of determining which connections will be allowed.
- A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users.

**Malicious Software:**

- Malicious logic is a set of instructions that cause a site's security policy to be violated.
- Malicious software, commonly known as malware, is any software that brings harm to a computer system.
- Malware can be in the form of worms, viruses, Trojans, spyware, adware and rootkits, etc., which steal protected data, delete documents or add software not approved by a user.
- Malware is software designed to cause harm to a computer and user.

**Viruses:**

- A computer virus is a program that inserts itself into one or more files and then performs some harmful action.
- A computer virus is a piece of software that can "infect" other programs by modifying them; the modification includes injecting the original program with a malicious code to make copies of the virus program, which can then go on to infect other programs.
- Whenever the infected computer comes into contact with an uninfected piece of software, a fresh copy of the virus passes into the new program.

**Worms:**

- A worm is a program that can replicate itself and send copies from computer to computer across network connections.
- Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function.
- A worm actively seeks out more machines to infect and each machine that is infected serves as an automated launching pad for attacks on other machines.
- Network worm programs use network connections to spread from system to system.

**Trojan Horse:**

- A Trojan horse is a program or command procedure containing hidden code that, when invoked, performs some unwanted or harmful function.
- A Trojan horse is any malware which misleads users of its true intent to fool a user into thinking it's a harmless file.
- Looks genuine, designed to trick the users.

**Antivirus:**

- The ideal solution to the threat of viruses is prevention: Do not allow a virus to get into the system in the first place, or block the ability of a virus to modify any files containing executable code or macros.
- This goal is, in general, impossible to achieve, although prevention can reduce the number of successful viral attacks.
- The next best approach is to be able to do the following:
    - **Detection:** Once the infection has occurred, determine that it has occurred and locate the virus.
    - **Identification:** Once detection has been achieved, identify the specific virus that has infected a program.
    - **Removal:** Once the specific virus has been identified, remove all traces of the virus from the infected program and restore it to its original state.

Antivirus software, also known as anti-malware, is a computer program used to prevent, detect, and remove malware. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.

Antivirus software begins operating by checking your computer programs and files against a database of known types of malware. Since new viruses are constantly created and distributed by hackers, it will also scan computers for the possibility of new or unknown types of malware threats.

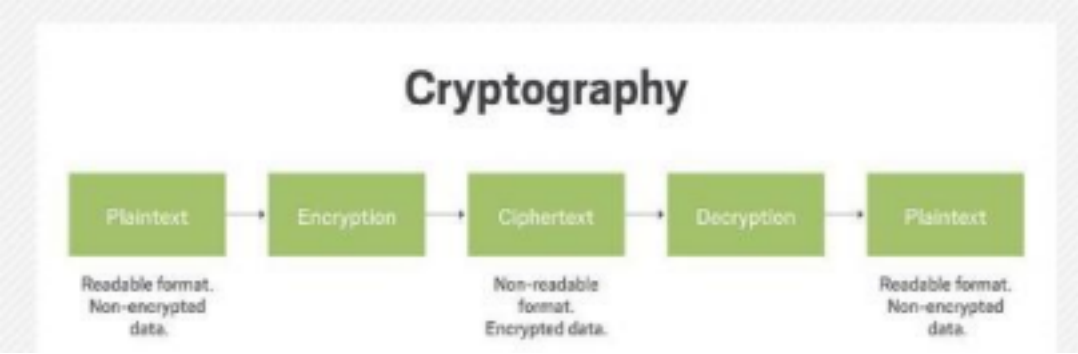
Features of Antivirus:

Features that make a good antivirus program are mentioned below:

- Malware Detection & Removal
- Firewall
- Auto Sandboxing Technique
- Virus Scan
- Identity protection
- Backup
- Email Protection
- Social media Protection

**Cryptography:**

Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it.




Encryption:

- Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.

Decryption:

- Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand (original form).
- It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

Plain text:

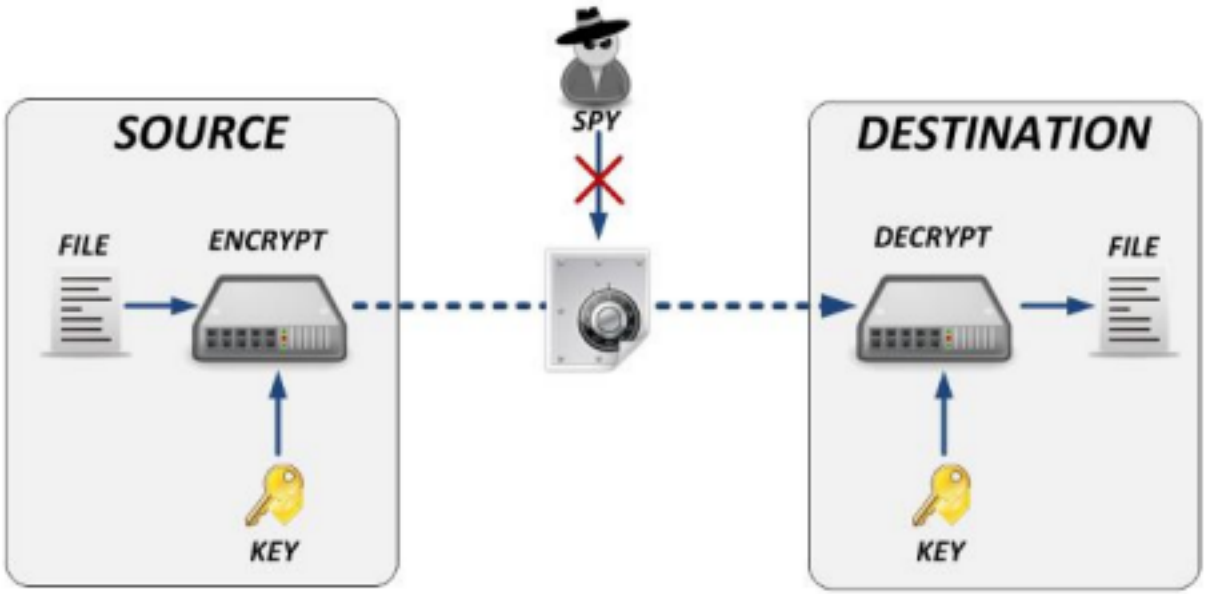
- Plaintext or cleartext is unencrypted information.

Cipher text:

- Ciphertext is encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result.

**Symmetric Key Cryptography/Secret Key Cryptography:**

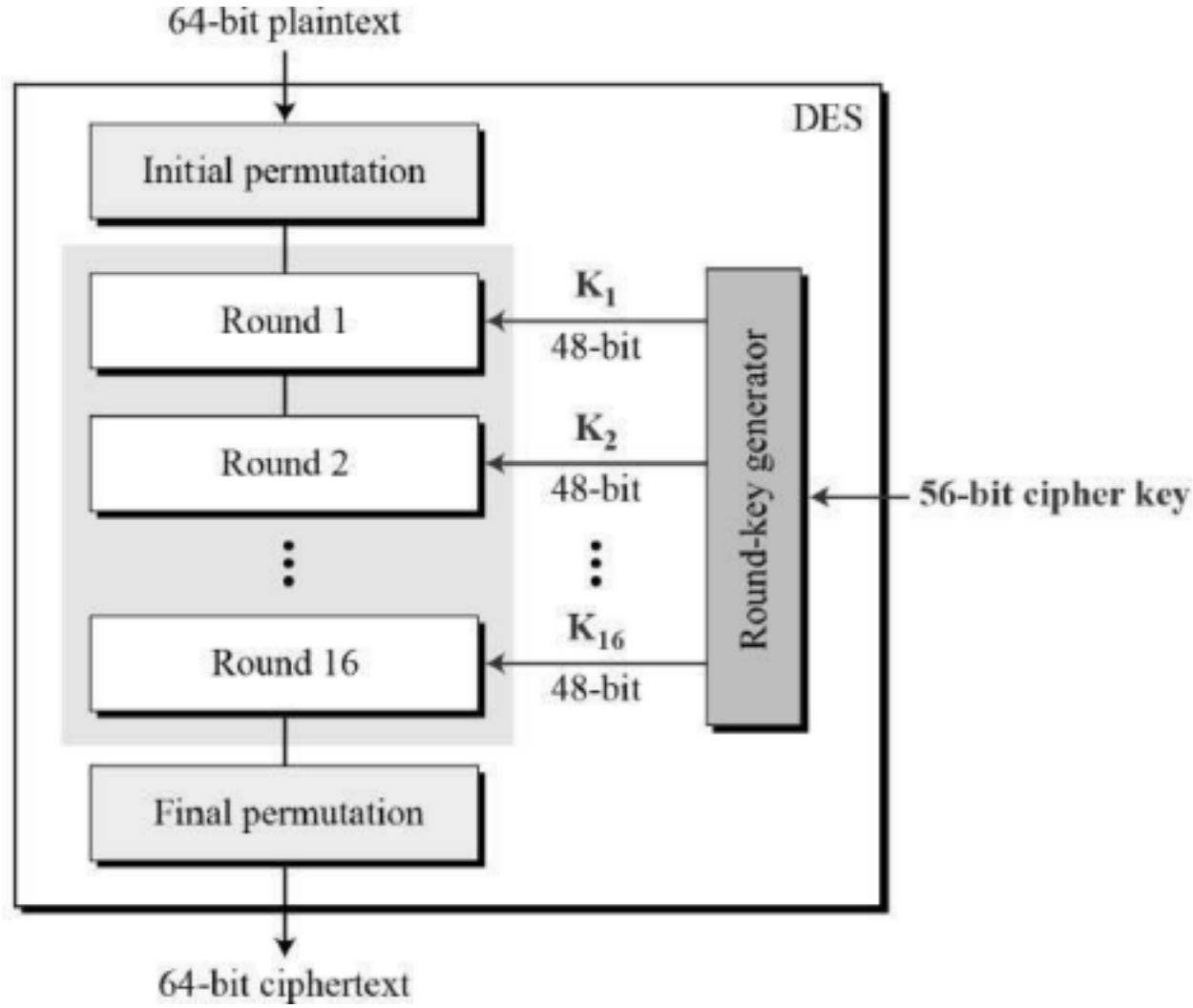
- Symmetric-key algorithms are the algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.
- Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way.




- Symmetric-key cryptography is sometimes called secret-key cryptography.
- The most popular symmetric-key system is the Data Encryption Standard (DES).

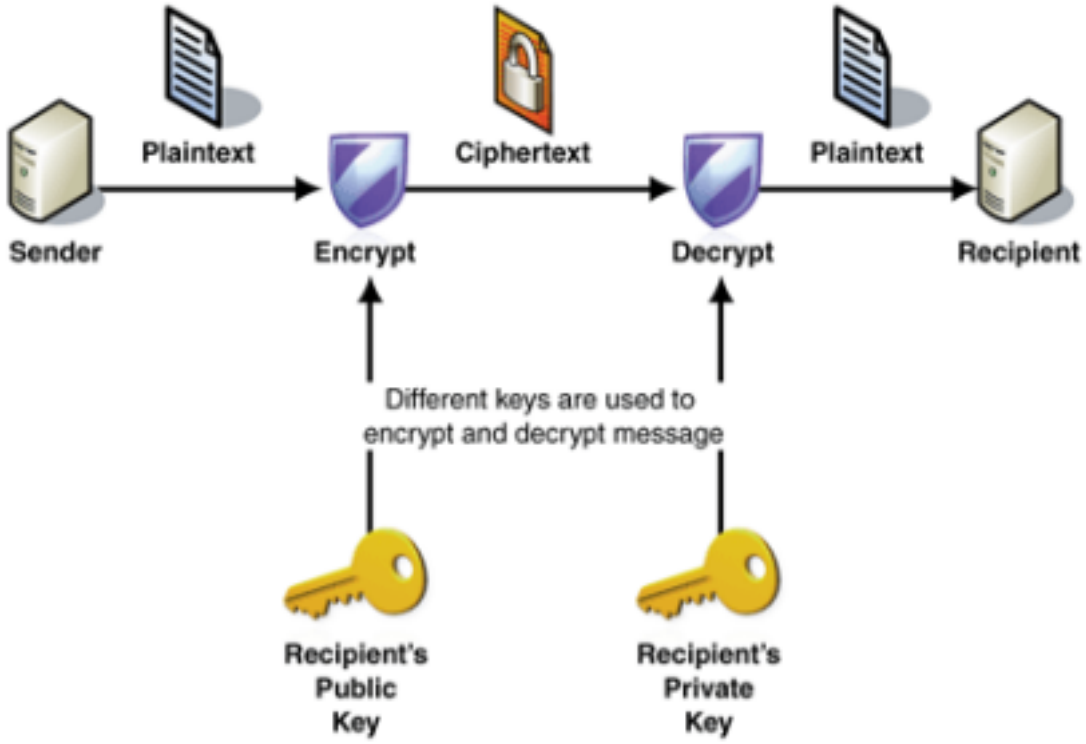
Data Encryption Standard:

- The Data Encryption Standard (DES) works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key.
- The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time.
- To encrypt a plaintext message, DES groups it into 64-bit blocks. Each block is enciphered using the secret key into a 64-bit ciphertext.
- The process involves 16 rounds and encrypting blocks individually or making each cipher block is dependent on all the previous blocks.




**Asymmetric key Cryptography/Public Key Cryptography:**

- Asymmetric cryptography, also known as Public key cryptography, uses public and private keys to encrypt and decrypt data.
- The keys are simply large numbers that have been paired together but are not identical (asymmetric).
- 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.




RSA Algorithm:

• RSA is one of the first public-key cryptosystems and is widely used for secure data transmission.

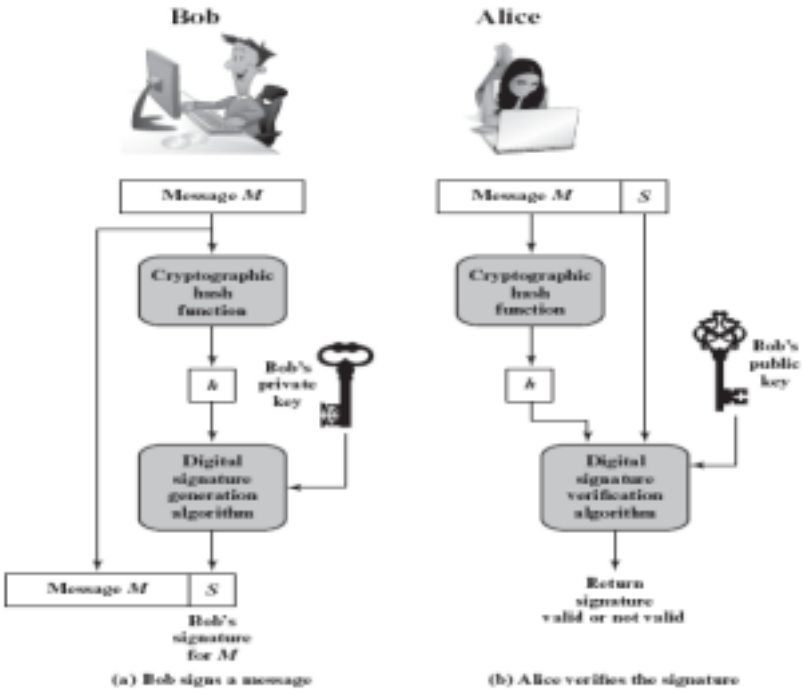
• In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret.

• The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption.

| Secret Key Cryptography | Public Key Cryptography |
|---|---|
| It uses a single key for both encryption and decryption, called a secret key. | It uses a different key for encryption and decryption, namely public key and private key respectively. |
| Symmetric encryption is fast in execution. | Asymmetric Encryption is slow in execution due to the high computational burden. |
| Old technique | Relatively new. |
| Less Secure | More Secure |
| Secret key should be delivered to the receiver. | Key delivery is not required. |

**Digital Signature:**

- A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature.
- A digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity.
- The signature guarantees the source and integrity of the message.
- Typically, the signature is formed by taking the hash of the message and encrypting the message with the creator’s private key.

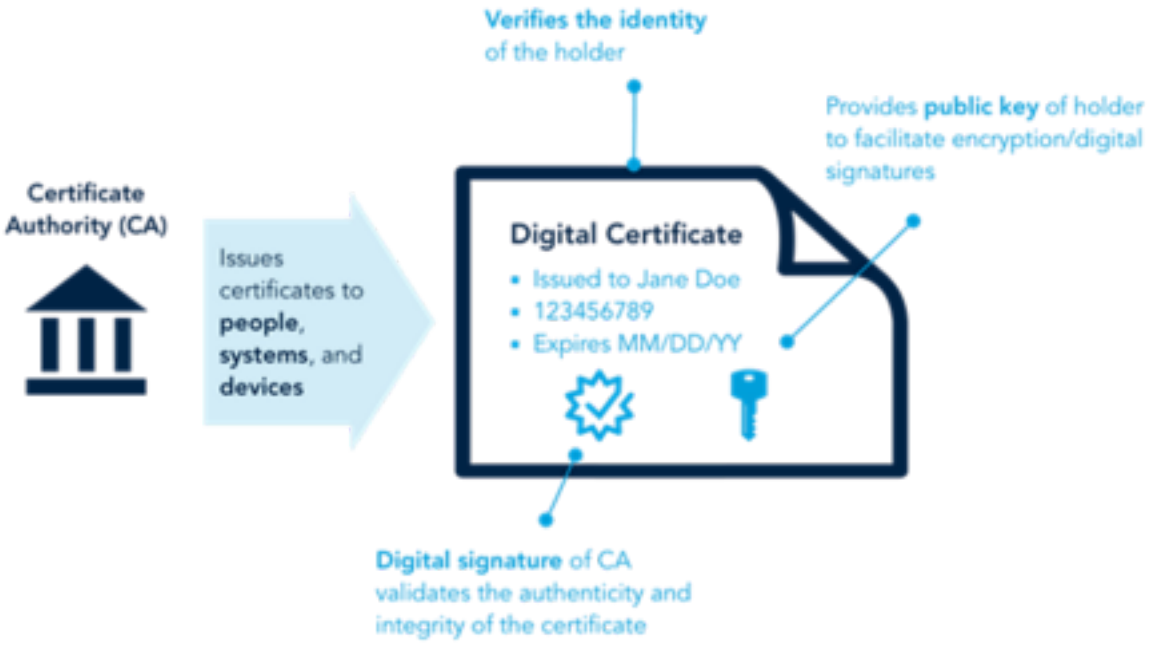


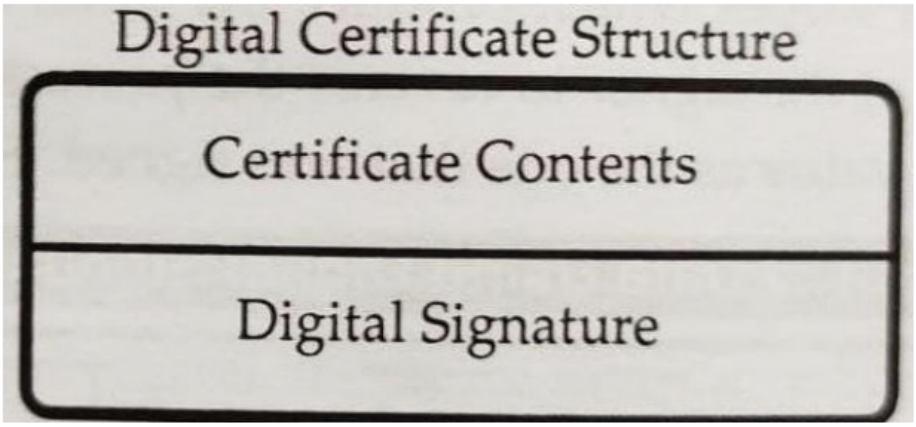
Types of Digital Signature:

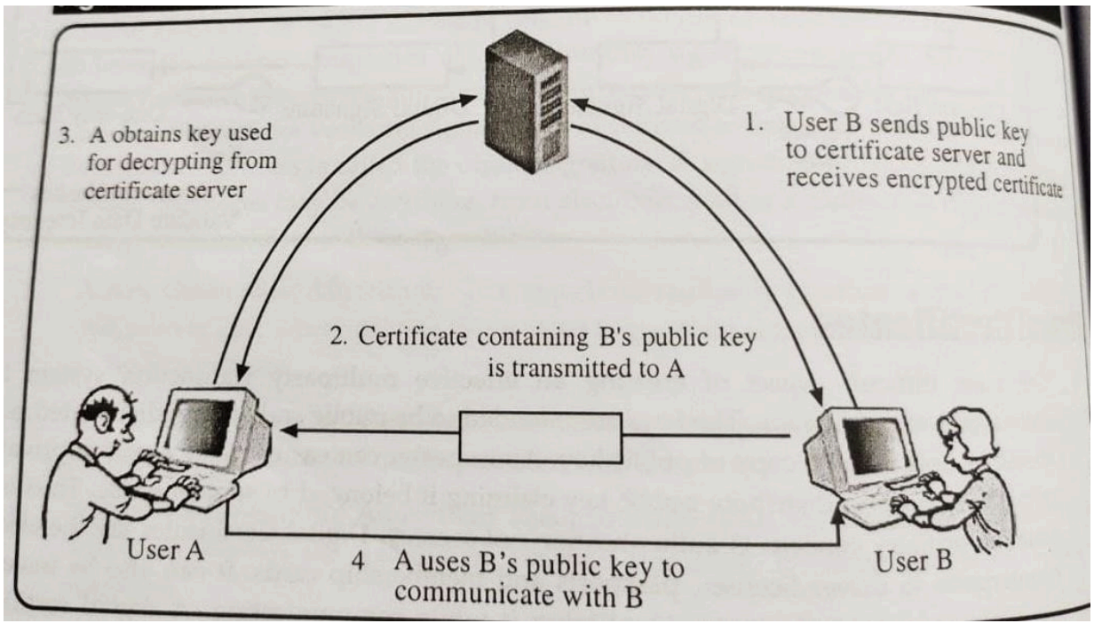
1. **Direct Digital Signature**
    - The term direct digital signature refers to a digital signature scheme that involves only the communicating parties (source, destination).
    - It is assumed that the destination knows the public key of the source.
    - Confidentiality can be provided by encrypting the entire message plus signature with a shared secret key (symmetric encryption).
    - Note that it is important to perform the signature function first and then an outer confidentiality function.
2. **Arbitrated Digital Signature**
    - Implementing an arbitrated digital signature invites a third party into the process called a "trusted arbiter."
    - The role of the trusted arbiter is usually twofold: first this independent third party verifies the integrity of the signed message or data.
    - Second, the trusted arbiter dates or time-stamps the document, verifying receipt and the passing on of the signed document to its intended final destination.

**Digital Certificate:**

- A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI). • A digital certificate may also be referred to as a public key certificate or identity certificate. • A digital certificate authenticates the Web credentials of the sender and lets the recipient of an encrypted message know that the data is from a trusted source (or a sender who claims to be one).
- A digital certificate is issued by a certification authority (CA).
- A person (sender), who is sending an encrypted message may obtain a digital certificate from a CA to ensure authenticity.
- The CA issues the digital certificate with the applicant's public key, along with other information such as holder name, serial number, date of expiration and a digital CA signature. • When a Web message is transmitted, a digital certificate serves as an encrypted attachment containing the public key and other relevant identifying data.
- The most common digital certificate standard is X.509 Certificate.



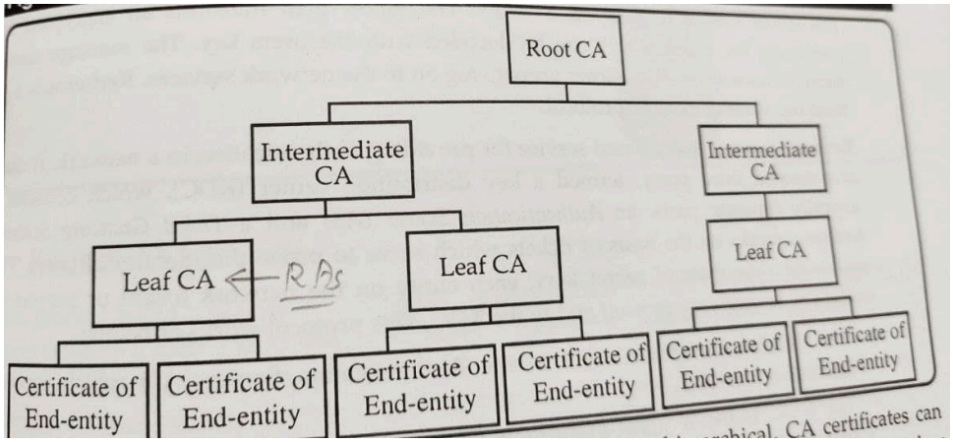

**Certificate Authority (CA):**

• A certificate authority (CA), also sometimes referred to as a certification authority, is a company or organization that is trusted to sign digital certificates.

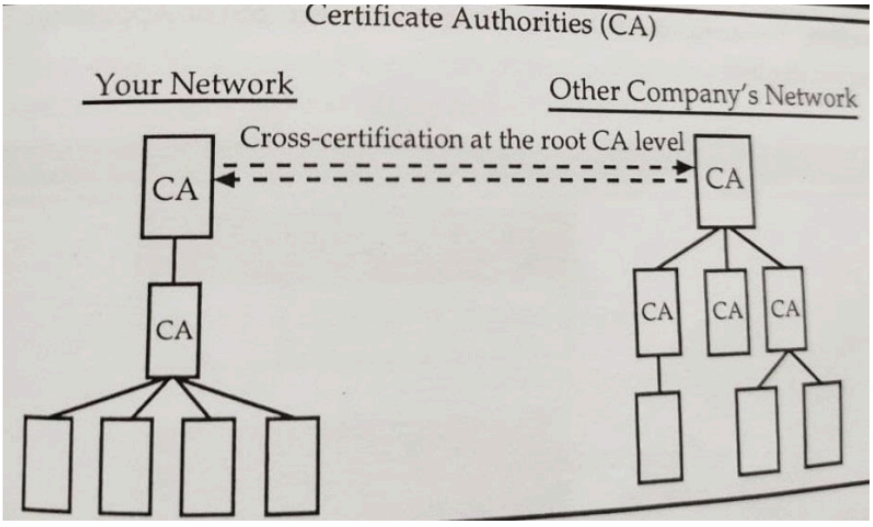
• CA verifies identity and legitimacy of company or individual that requested the certificate and if the verification is successful, CA issues signed certificate.

• CA is responsible for managing all aspects of digital certificate issuance, publication, revocation, renewal etc.

• Every digital certificate usually can be chained to a Root CA, which is the final trust point. • The root CA then issues a certificate to one or more subordinate CAs, and again these intermediate CAs to Leaf CAs (also called as Registration Authorities RAs) and RAs are responsible to issue the certificate to end entities.



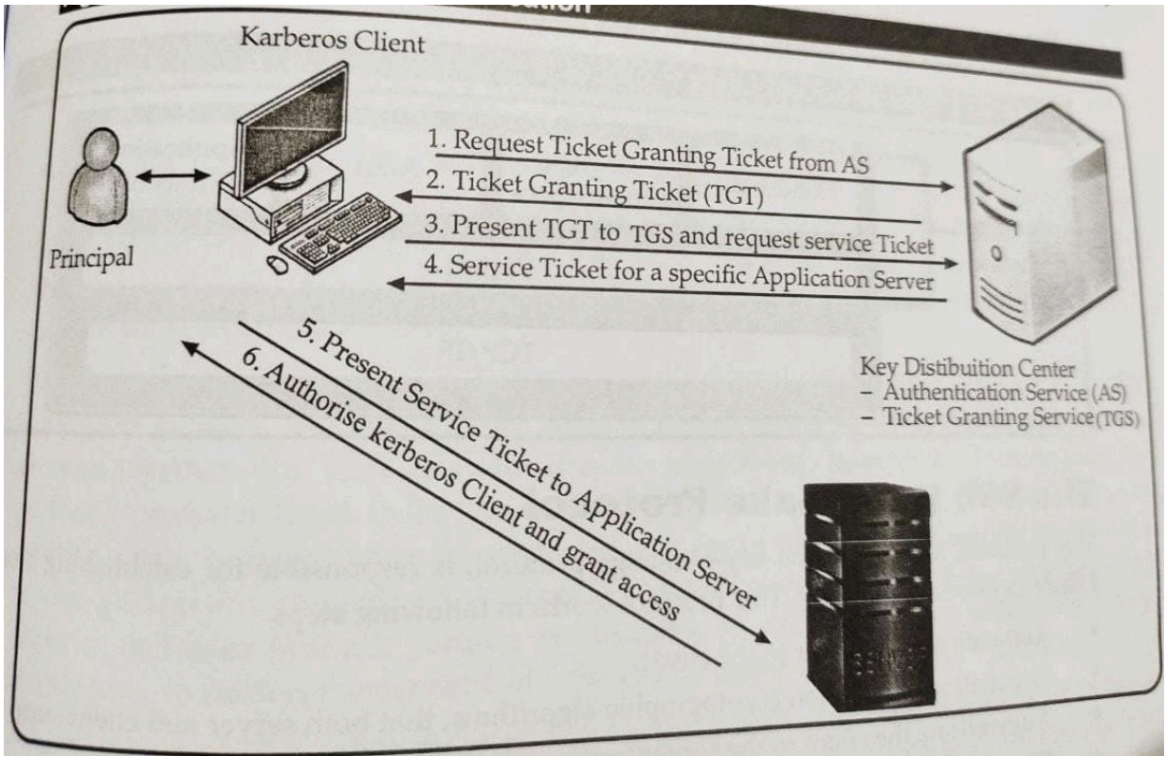

• Although the relationship between CAs is most commonly hierarchical, CA certificates can also be used to establish trust relationships between CAs in two different public key infrastructure (PKI) hierarchies.



**Third Party Authentication:**

- Authentication means verifying the identity of someone who wants to access data, resources, or applications.
- Validating that identity establishes a relationship for further interactions. The verifier demands assurance of the identity of the user (referred to as client/principal).
- Password based systems are a widely used technique to achieve authentication. But the main problem still with password-based systems is that it can be collected by eavesdroppers during transmission through network which can be made difficult by encrypting passwords but still online and offline password guessing attacks are possible.
- In the third-party authentication systems, the password or encryption key itself never travels over the network. Rather an authentication server maintains a file of obscure facts about each registered user.
- At the log-on time, the server computes a token. The server then transmits an encrypted message containing the token, which can be decoded with the user's key.
- The message contains an authentication token that allows users to log on to the network services.
- Kerberos is a popular third-party authentication protocol.
- Kerberos is a secret key based service for providing authentication in a network. It makes use of a trusted third party, termed a key distribution center (KDC), which consists of two logically separate parts: An Authentication Server (AS) and a Ticket Granting Server (TGS).
- Kerberos works on the basis of tickets which serve to prove the identity of users. The KDC maintains a database of secret keys; each entity on the network (client or server) shares a secret key known only to itself and to the KDC.
- This protocol works as below:
    - The client authenticates itself to the Authentication Server (AS) which forwards the username to a KDC.
    - The KDC issues a ticket-granting ticket (TGT) and sends it to the client in the form of an encrypted message.
    - Once the client receives messages, the client decrypts it and sends the TGT to the ticket granting service (TGS).
    - After verifying the TGT is valid, the TGS issues a ticket and session keys, which are returned to the client.
    - The client then sends the ticket to the service server (SS) or Application Server along with

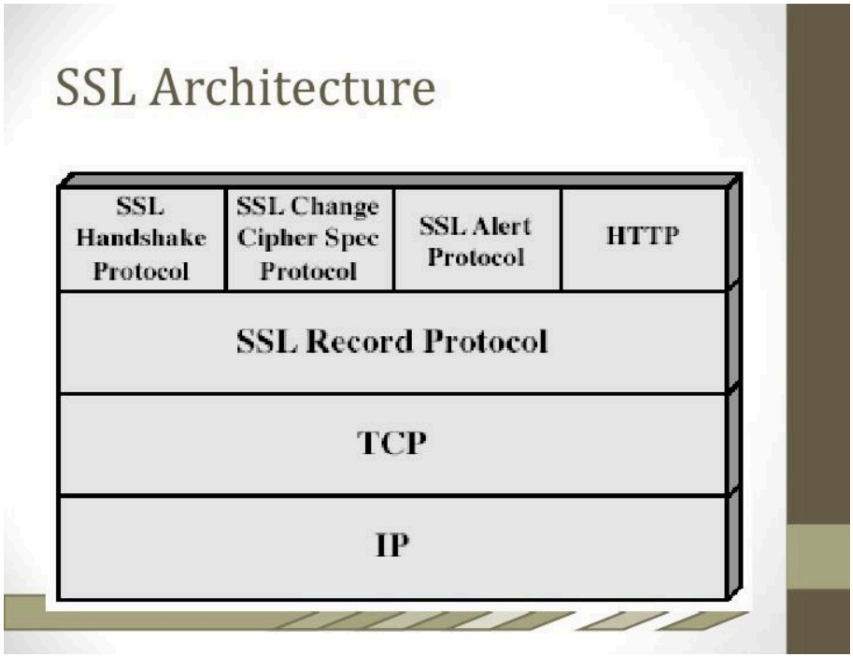
its service request.




**Secure Socket Layer (SSL):**

- Secure Sockets Layer (SSL) is a standard protocol used for the secure transmission of documents over a network.
- Developed by Netscape, SSL technology creates a secure link between a Web server and browser to ensure private and integral data transmission.
- SSL uses Transport Control Protocol (TCP) for communication.
- In SSL, the word socket refers to the mechanism of transferring data between a client and server over a network.
- When using SSL for secure Internet transactions, a Web server needs an SSL certificate to establish a secure SSL connection.
- The objectives of SSL are:
    - Data integrity: Data is protected from tampering.
    - Data privacy: Data privacy is ensured through a series of protocols, including the SSL Record Protocol, SSL Handshake Protocol, SSL Change CipherSpec Protocol and SSL Alert Protocol.
    - Client-server authentication: The SSL protocol uses standard cryptographic techniques to authenticate the client and server.

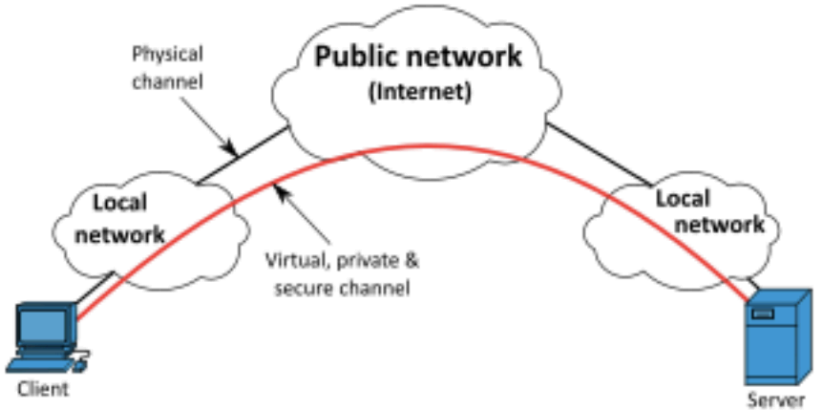
Architecture of SSL:




- SSL Handshake protocol: This protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in an SSL record.
- SSL Record Protocol: The SSL Record Protocol provides basic security services to higher layer protocols.
- SSL Change Cipher Spec Protocol: Change Cipher Spec messages are used in SSL to indicate that the communication is shifted from unencrypted form to encrypted form. Or, in other words, the other communicating party is informed about the security mechanism being used. • SSL Alert Protocol: The Alert Protocol is used to convey SSL related alerts to the peer entity.

**Virtual Private Network (VPN):**

- A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network.
- The encrypted connection helps ensure that sensitive data is safely transmitted. • It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.
- VPN technology is widely used in corporate environments.
- A VPN extends a corporate network through encrypted connections made over the Internet. • Because the traffic is encrypted between the device and the network, traffic remains private as it travels.
- An employee can work outside the office and still securely connect to the corporate network.

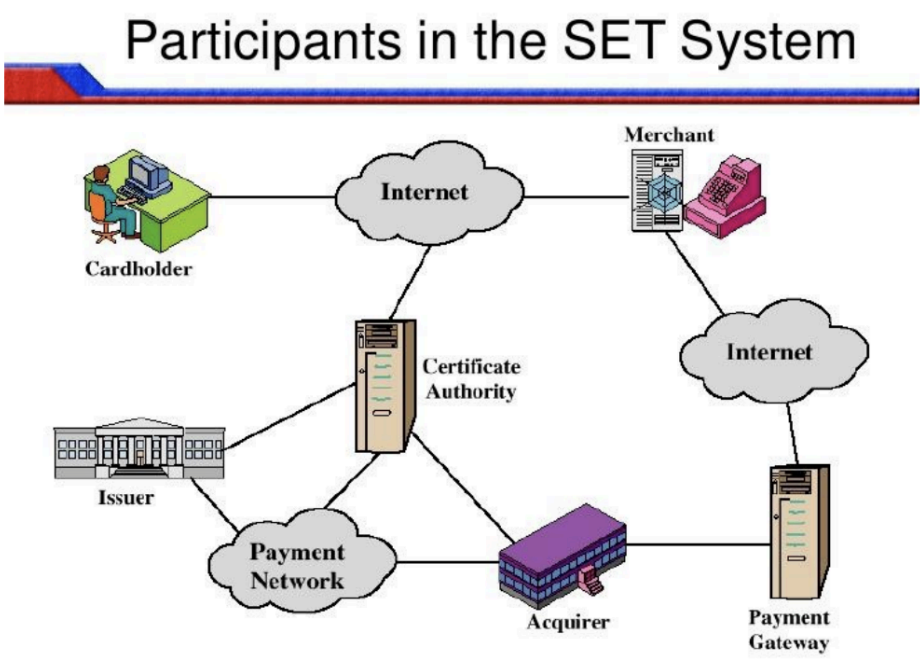



Types of VPNs:

1. Remote Access
    - A remote access VPN securely connects a device outside the corporate office. These devices are known as endpoints and may be laptops, tablets, or smartphones.
    - Advances in VPN technology have allowed security checks to be conducted on endpoints to make sure they meet a certain security criterion before connecting.
    - Think of remote access as a computer to a network.
2. Site to Site
    - A site-to-site VPN connects the corporate office to branch offices over the Internet. • Site-to-site VPNs are used when distance makes it impractical to have direct network connections between these offices.
    - Dedicated equipment is used to establish and maintain a connection. Think of site-to-site access as network to network.

**Secure Electronic Transaction:**

- A secure electronic transaction (SET) is an open-source and cryptography-based protocol for secure payment processing via a non-secure network.
- In 1996, SET was launched and backed by VISA, MasterCard and other payment processing industry leaders.
- SET's algorithm ensures data confidentiality, data integrity and cardholder/merchant authentication.
- An SET system includes the following components:
    - Merchant
    - Cardholder/acquirer
    - Card issuer
    - Payment gateway
    - Certification authority (CA)
    - Dual signature: A guaranteed SET data integrity innovation that links two different recipient messages



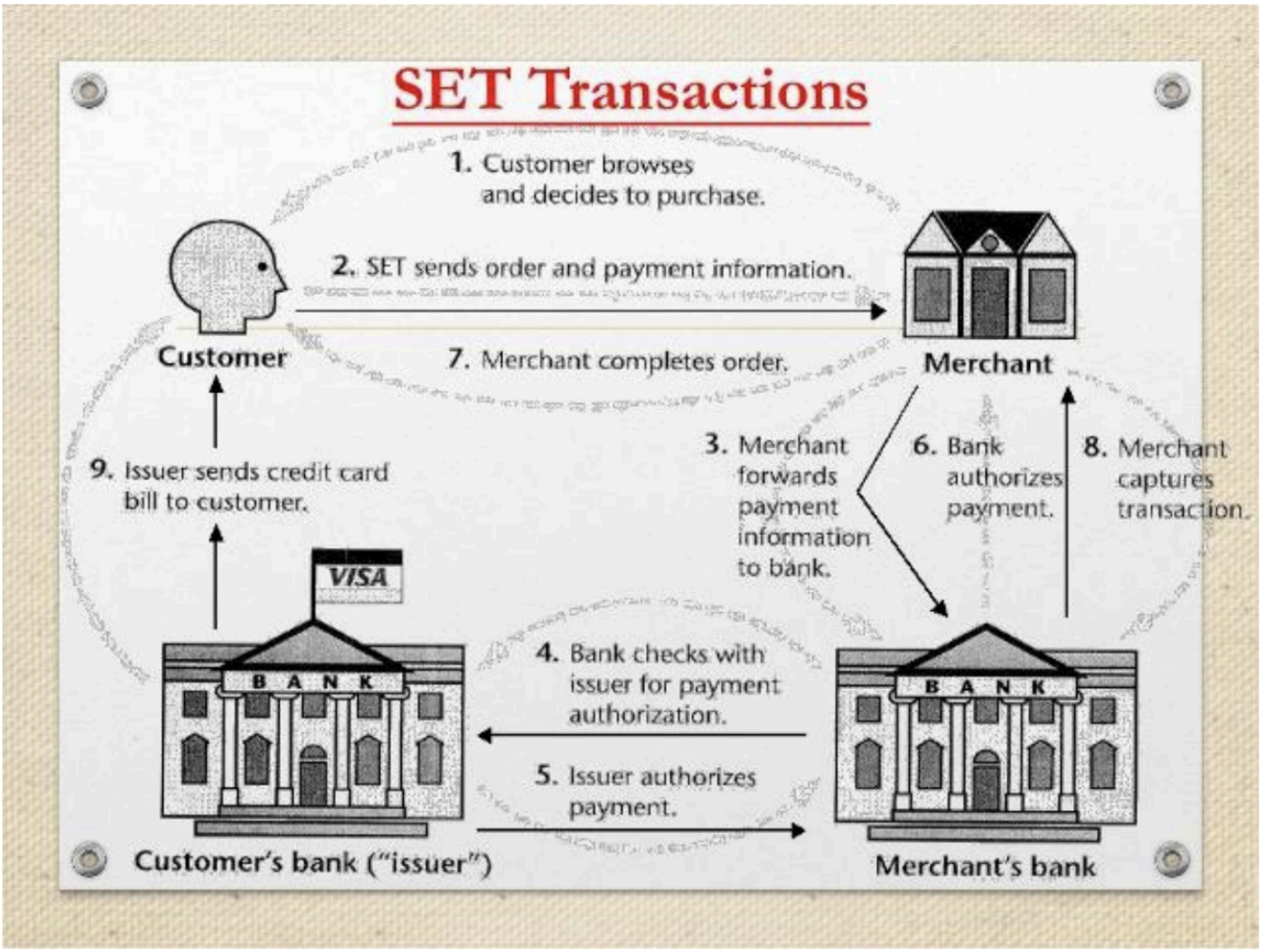

SET protocol provides three services:

• Provides a secure communication channel among all parties involved in a transaction • Provides trust by use of digital certificates

• Ensure privacy because the information is only available to parties in a transaction when and where necessary

Working of SET:

• The customer opens an account
• The customer receives a certificate
• Merchants have their own certificates
• The customer places an order
• The merchant is verified
• The order and payment information are sent by customer
• The merchant requests payment authorization
• The merchant confirms the order
• The merchant ships the ordered item
• The merchant requests payment through payment gateway


SET Transactions
1. Customer browses and decides to purchase.
2. SET sends order and payment information.
Customer
7. Merchant completes order.
Merchant
3. Merchant forwards payment information to bank.
6. Bank authorizes payment.
8. Merchant captures transaction.
9. Issuer sends credit card bill to customer.
VISA
BANK
4. Bank checks with issuer for payment authorization.
5. Issuer authorizes payment.
BANK
Customer's bank ("issuer")
Merchant's bank