

Unit-5

Internet infrastructure

- Internet infrastructure is the **physical hardware, transmission media, and software used to interconnect computers and users on the Internet**. Internet infrastructure is responsible for hosting, storing, processing, and serving the information that makes up websites, applications, and content
- Various internet infrastructures are:
 - TCP/IP
 - DNS
 - Border Gateway Protocol etc.

TCP/IP model

- the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols.
- It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model.

- The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer(ARP)

1. Network Access Layer -

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.

We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

2. Internet Layer –

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **IP** – stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP** – stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **ARP** – stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

- **3. Host-to-Host Layer –**

- This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :
 - TCP
 - UDP

1. **Transmission Control Protocol (TCP)** – It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP)** – On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

- **4. Application Layer –**

- This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP etc.

TCP/IP MODEL

Application Layer

Transport Layer

Internet Layer

Network Access Layer

OSI MODEL

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

Difference between TCP/IP and OSI Model.

TCP/IP

TCP refers to Transmission Control Protocol.

TCP/IP has 4 layers.

TCP/IP is more reliable

TCP/IP does not have very strict boundaries.

TCP/IP follow a horizontal approach.

OSI

OSI refers to Open Systems Interconnection.

OSI has 7 layers.

OSI is less reliable

OSI has strict boundaries

OSI follows a vertical approach.

TCP/IP uses both session and presentation layer in the application layer itself.

OSI uses different session and presentation layers.

TCP/IP developed protocols then model.

OSI developed model then protocol.

Transport layer in TCP/IP does not provide assurance delivery of packets.

In OSI model, transport layer provides assurance delivery of packets.

TCP/IP model network layer only provides connection less services.

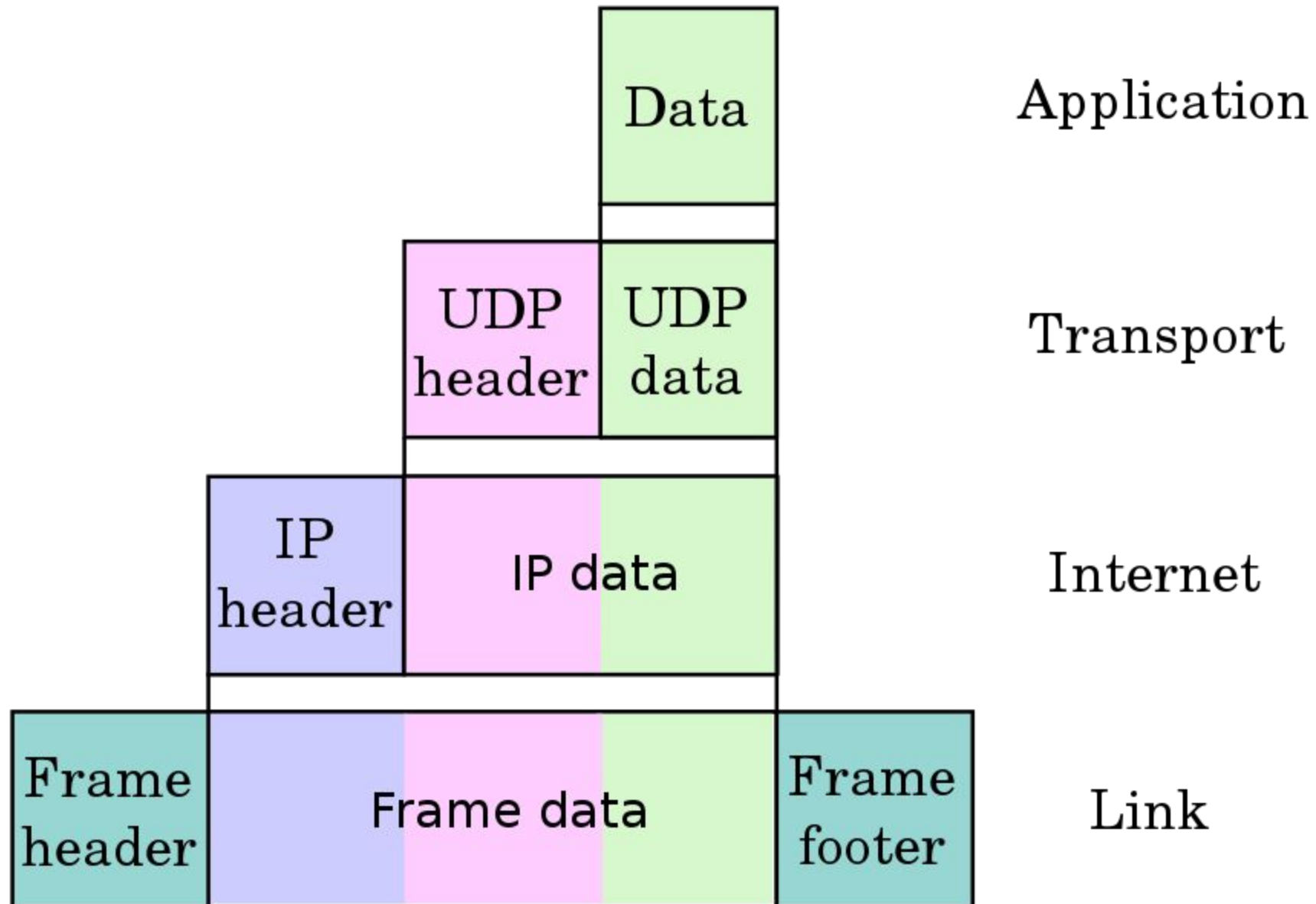
Connection less and connection oriented both services are provided by network layer in OSI model.

Internet protocol

The Internet Protocol is responsible for addressing [host interfaces](#), encapsulating data into datagrams (including [fragmentation and reassembly](#)) and routing datagrams from a source host interface to a destination host interface across one or more IP networks.

Four functions of IP are:

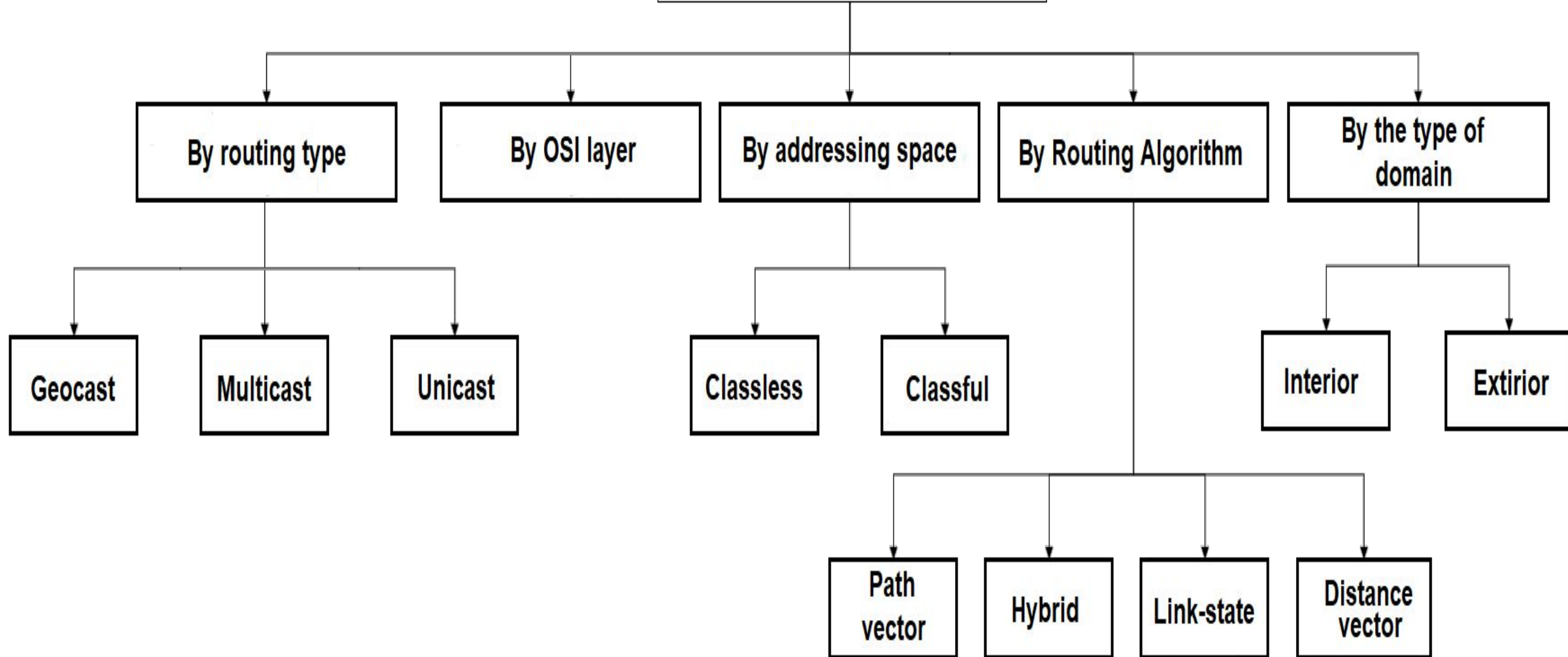
- Addressing
- Data Encapsulation and formatting
- Fragmentation and reassembly
- Routing/Indirect Delivery



Routing protocol

- A **routing protocol** specifies how routers communicate with each other to distribute information that enables them to select routes between nodes on a computer network.

**Classification of routing protocol in
the fixed data networks**



Internal Gateway Protocol (IGP)

RIP

OSPF

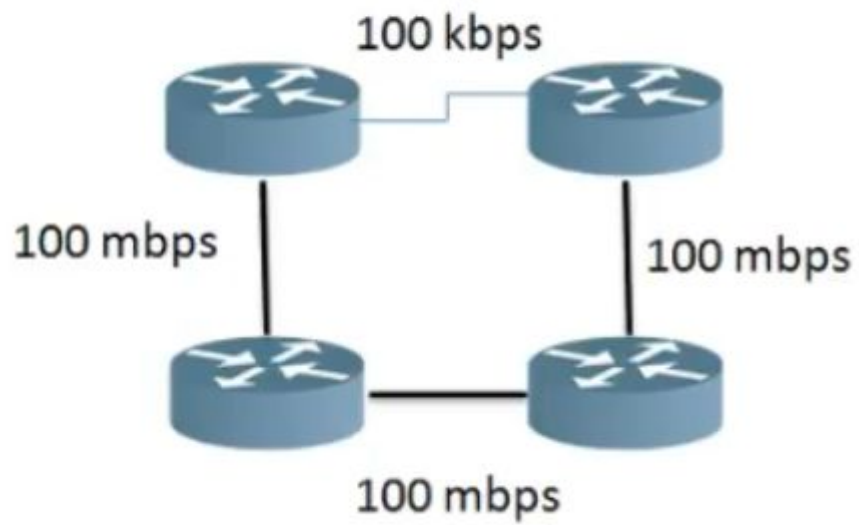
EIGRP

External Gateway Protocol (EGP)

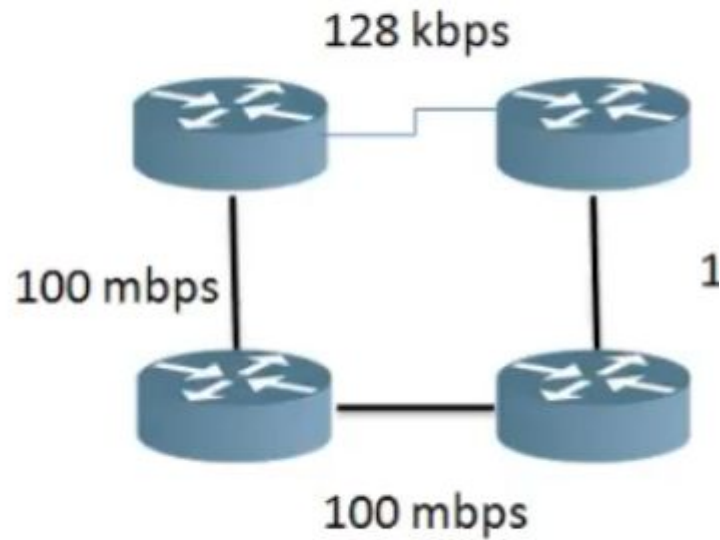
BGP

EGP

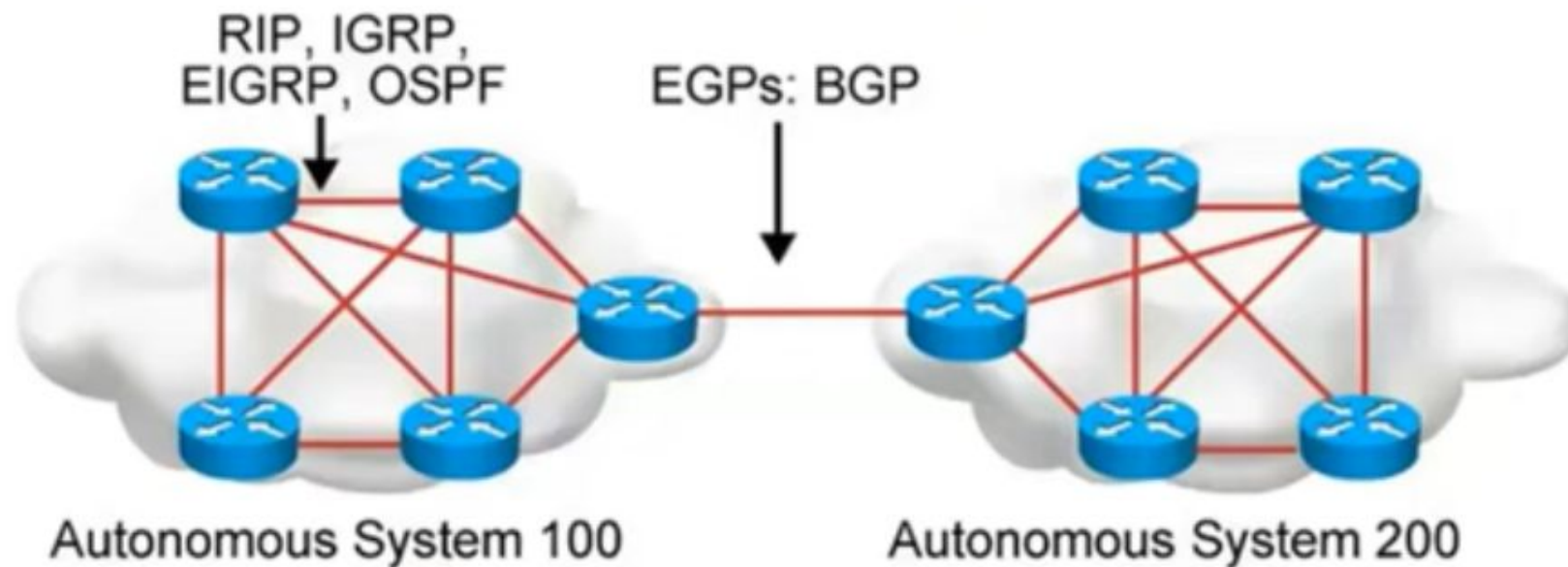
DISTANCE Vector



LINK State

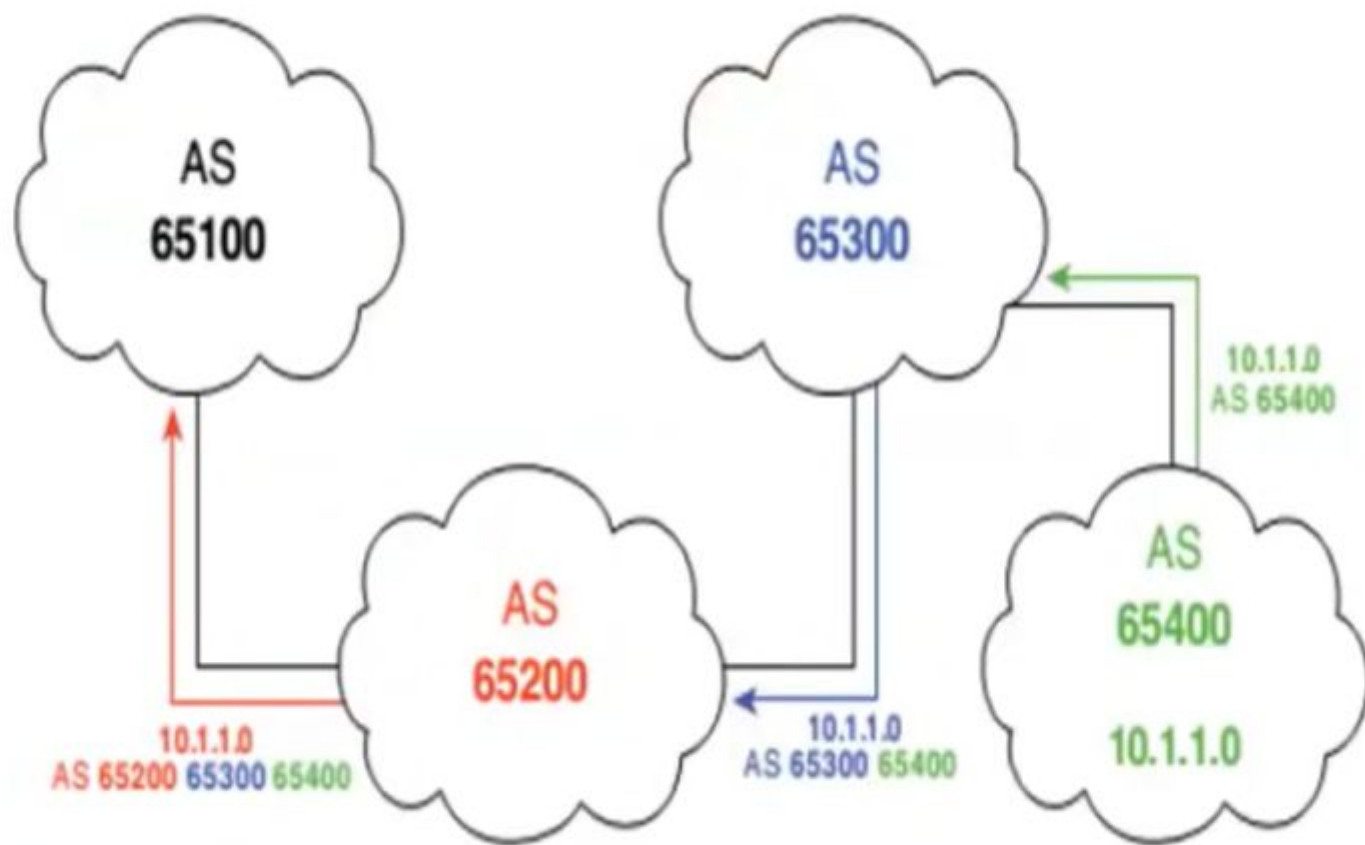


BGP Autonomous Systems



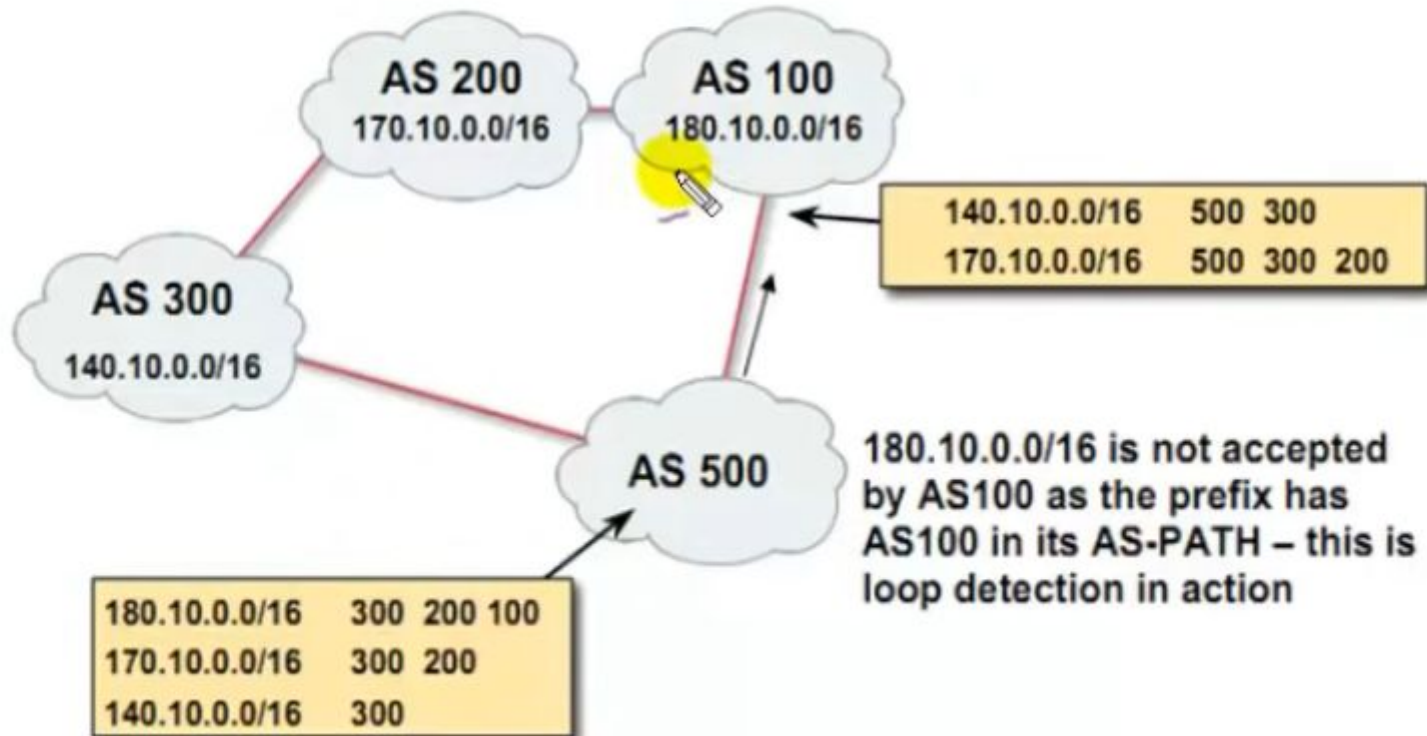
- ▶ *An AS is a collection of networks under a single technical administration.*
- ▶ *IGPs operate within an AS.*
- ▶ *BGP is used between autonomous systems.*
- ▶ *Exchange of loop-free routing information is guaranteed.*

Path Vector

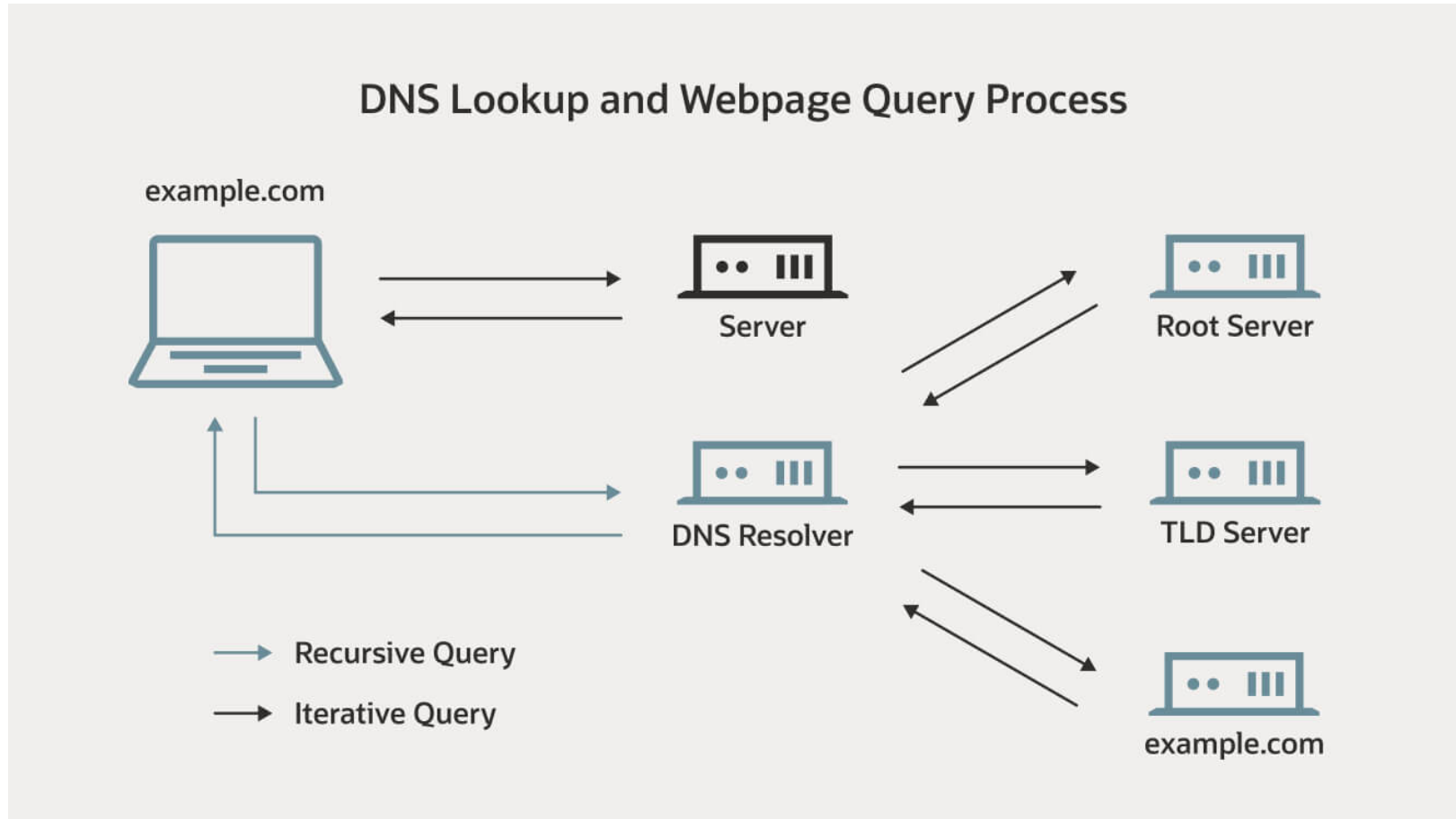


BGP's loop prevention mechanism

AS-Path loop detection



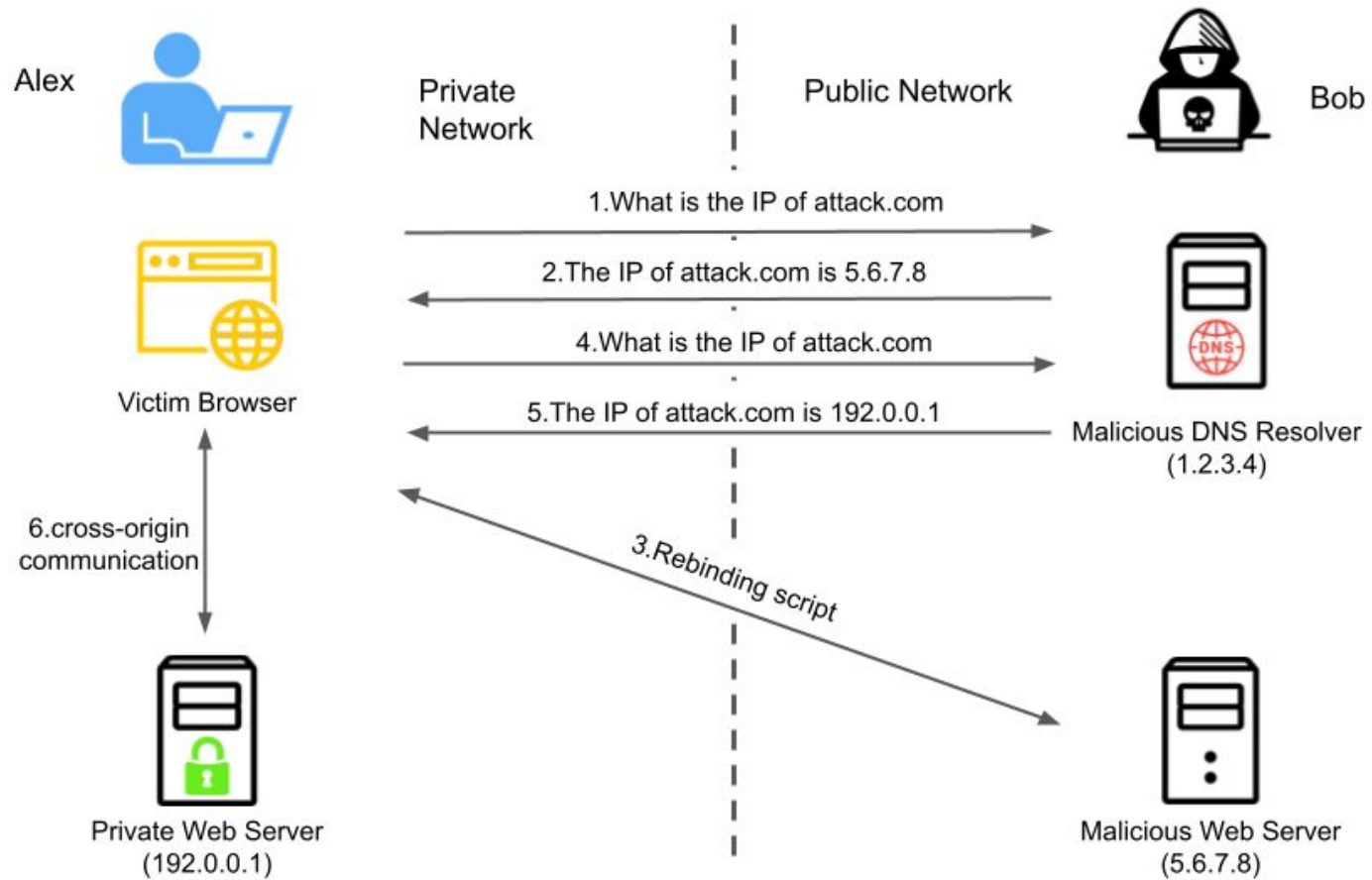
DNS(domain name system)



DNS rebinding

- DNS rebinding is a method of manipulating resolution of domain names that is commonly used as a form of computer attack. In this attack, a malicious web page causes visitors to run a client-side script that attacks machines elsewhere on the network.

DNS Rebinding



Key Management

- The main aim of key management is to generate a secret key between two parties and store it to prove the authenticity between communicating users.
- Key management is the techniques which support **key generation, storage and maintenance of the key** between authorized users.
- Key management plays an important role in cryptography as the basis for securing cryptographic goals like **confidentiality, authentication, data integrity** and **digital signatures**.
- It is not the case where communicating parties are using same key for encryption and decryption or whether two different keys are used for encryption and decryption.

Key management

What is Key Management?

- ★ Key management is the management of cryptographic keys in a cryptosystem.
- ★ This includes dealing with the generation, exchange, storage, use, and replacement of keys.
- ★ It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.
- ★ It deals with entire key lifecycle.

Why are we talking about key management?

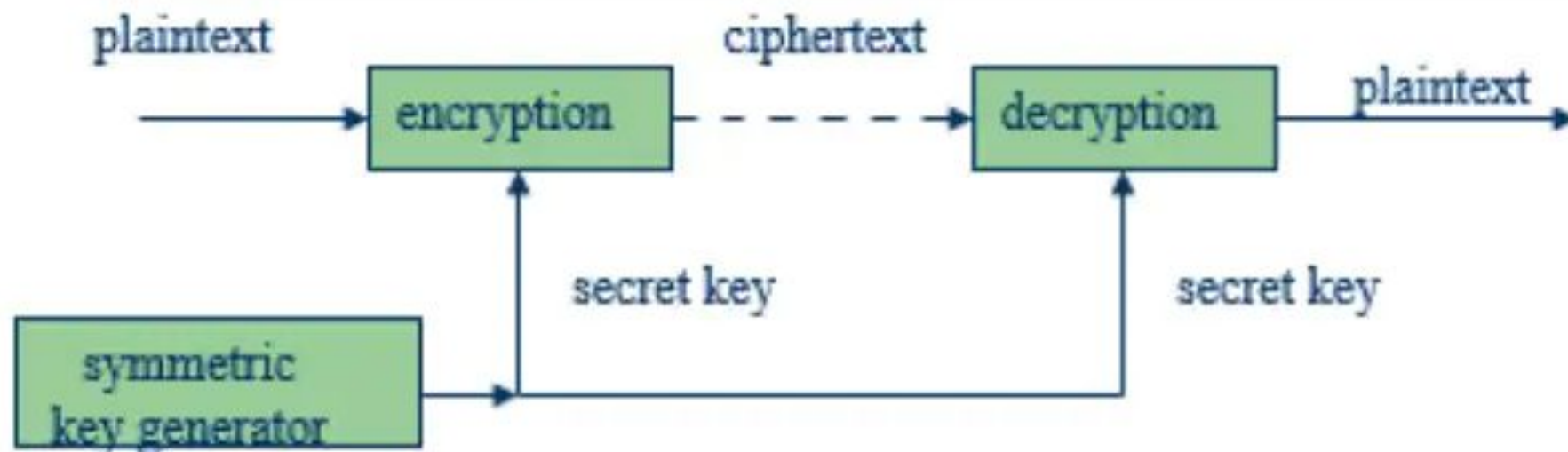
★ With the rise of Cybercrime, companies are investing significant amounts in Information Security in order to protect themselves, their employees and partners, but in the end that might not be enough.

★ Threats:

- compromise of confidentiality of secret keys
- compromise of authenticity of secret or public keys.
- unauthorized use of public or secret keys

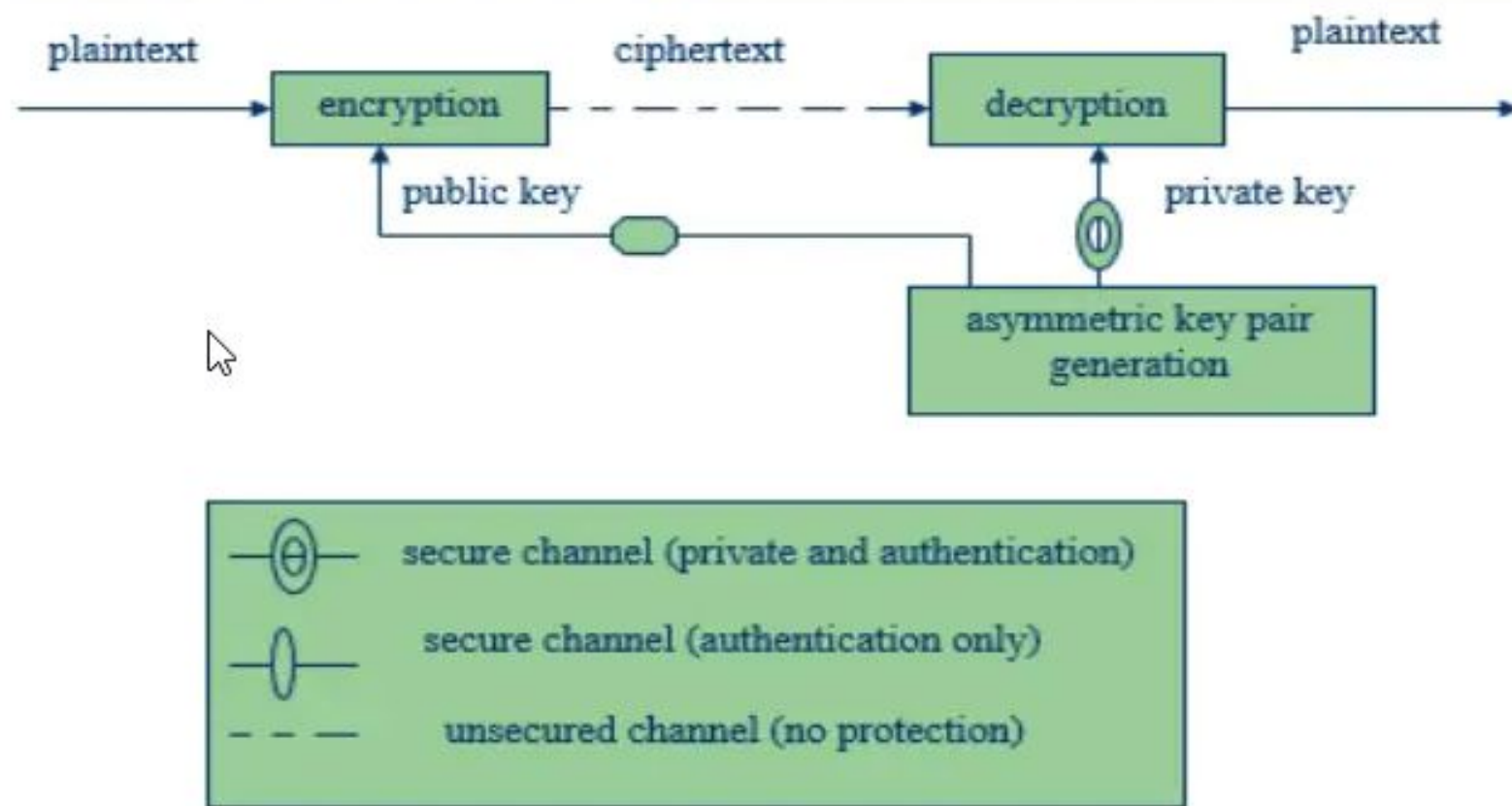
Key management techniques

a) Symmetric-key encryption:

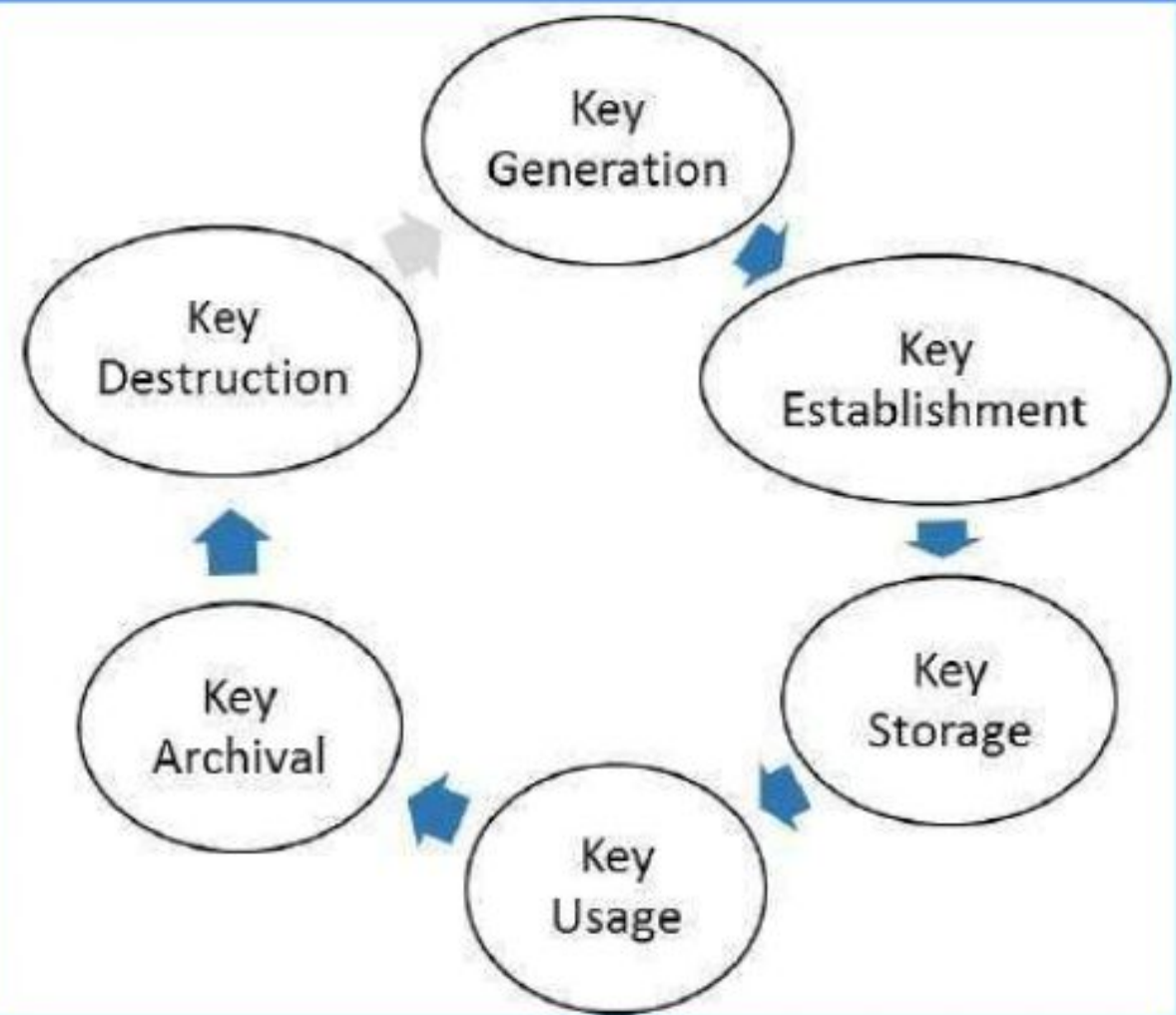



Key management techniques

b)Public-key encryption:



Key LifeCycle





Distribution of Public Keys

- ★ Public announcement
- ★ Publicly available directory
- ★ Public-key authority
- ★ Public-key certificates

