Application Layer Protocols

&

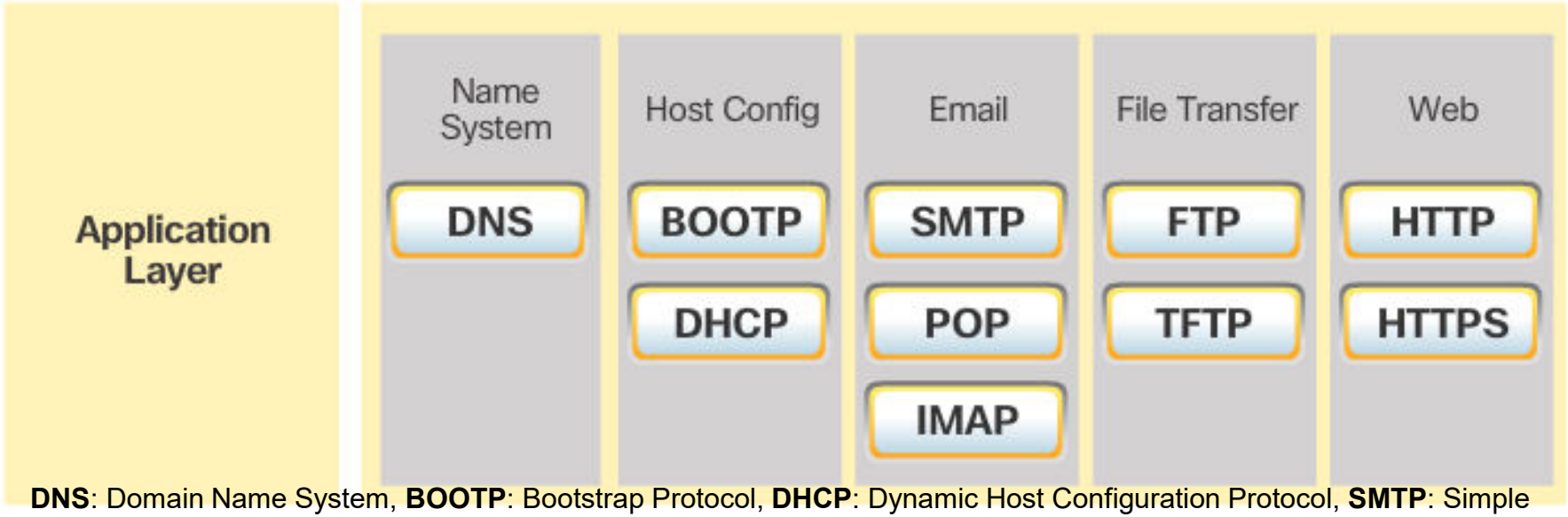
Basics of Network Security

Application Layer

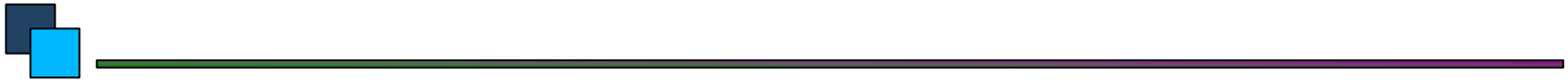
- Closest to the end user.
- Application layer protocols help exchange data between programs running on the source and destination hosts.
- The TCP/IP application layer performs the functions of the upper three layers of the OSI model.
- Common application layer protocols include HTTP, FTP, TFTP(Trivial FTP), DNS.

Application Layer Protocols

- TCP/IP Application Layer Protocols
  - TCP/IP application protocols specify the format and control information necessary for common Internet functions.
  - Application layer protocols must be implemented in both the source and destination devices.
  - Application layer protocols implemented on the source and destination host must be compatible to allow communication



DNS: Domain Name System, **BOOTP**: Bootstrap Protocol, **DHCP**: Dynamic Host Configuration Protocol, **SMTP**: Simple Mail Transfer Protocol, **POP**: Post Office Protocol, **IMAP**: Internet Message Access Protocol, **FTP**: File Transfer Protocol, **TFTP**: Trivial File Transfer Protocol, **HTTP**: Hypertext Transfer Protocol, **HTTPS**: Hypertext Transfer Protocol Secure



INTERNET APPLICATIONS

Internet Applications

We will cover

- Domain Name Service

→ DNS

- Proxy Service

→Squid Proxy, Apache Proxy Server

- Mail Service

→SMTP, POP, IMAP

- Web Service

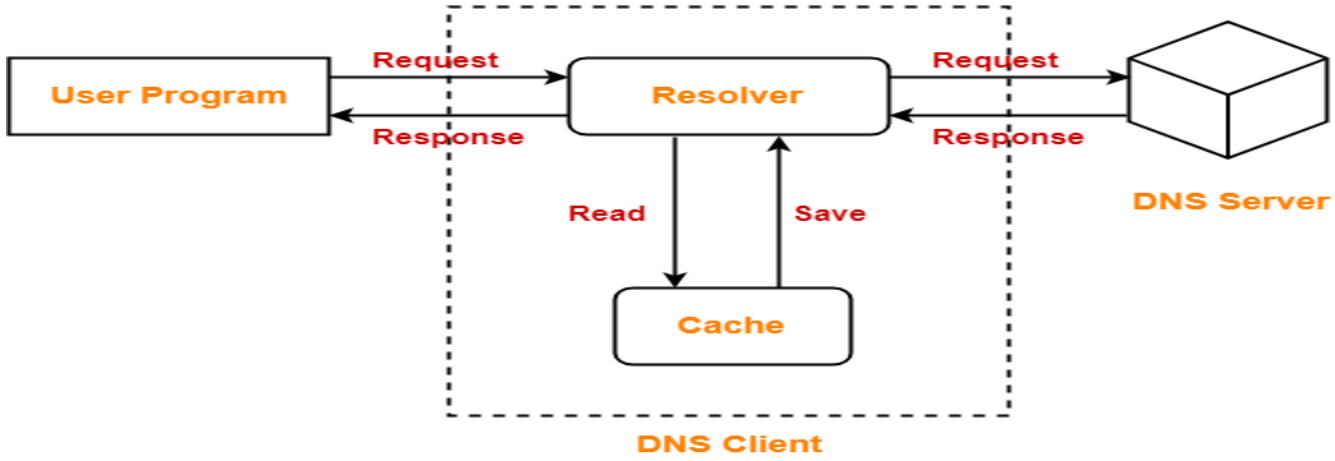
→ HTTP, HTTPS

Besides these…

SL	Application
File Sharing Service	FTP, BitTorrent
Remote Access Service	Telnet, SSH, RDP
Streaming Service	YouTube, Netflix, Spotify
VoIP Service	Skype, Zoom, WhatsApp
Instant Messaging Service	WhatsApp, Slack, Microsoft Teams
Online Gaming Service	Xbox Live, Steam, PlayStation Network
Cloud Storage Service	Google Drive, Dropbox, OneDrive
Social Networking Service	Facebook, Twitter, LinkedIn
E-commerce Service	Amazon, eBay, Alibaba
Search Engine Service	Google Search, Bing, DuckDuckGo
VPN Service	NordVPN, ExpressVPN

DNS

- DNS is short for Domain Name Service or Domain Name System.
- DNS is a host name to IP Address translation service
- It converts the names we type in our web browser address bar to the IP Address of web servers hosting those sites
- The following diagram illustrates the process of DNS resolution-



DNS Operation

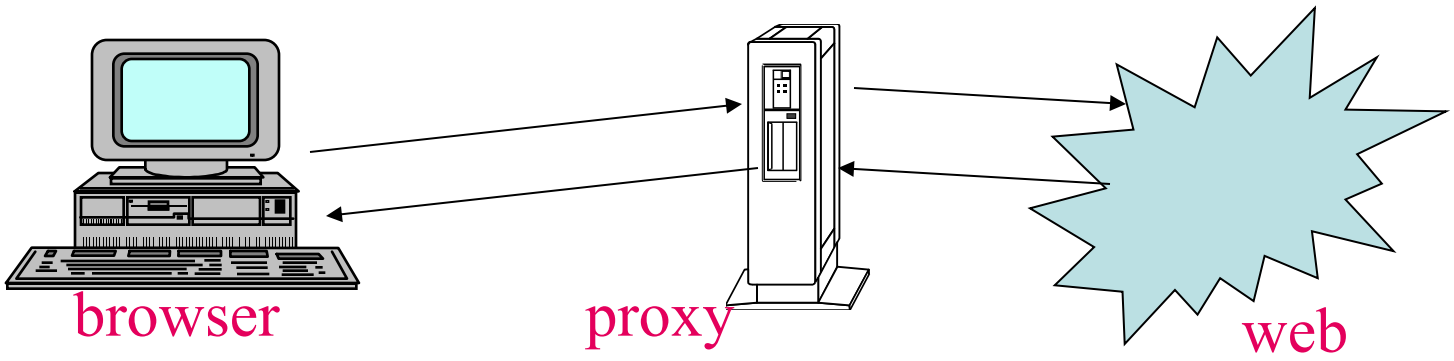
- A DNS server maintains the name to IP address mapping of the domain for which it is the name server.
- The DNS server for a domain is registered with the domain registrar and the entry is maintained by the Internet Root-Servers or Country Level Root-Servers.
- Whenever a server is asked, if doesn't have the answer, the root servers are contacted.
- The root servers refer to the DNS server for that domain (in case the domain is a top-level domain) or the Country Root Server (in case the domain is country level domain).

PROXY SERVER

- In computer networking, a proxy server is a server application or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources
- Instead of connecting directly to a server that can fulfill a requested resource (such as: a file or web page), the client directs the request to the proxy server, which evaluates the request and performs the required network transactions.

What is a Web Proxy?

- A proxy is a host which relays web access requests from clients
  - Used when clients do not access the web directly
  - Used for security, logging, accounting and performance



What is Web Caching?

- Storing copies of recently accessed web pages
- Pages are delivered from the cache when requested again

- Browser caches
- Proxy caches

Why Cache?

- Shorter response time
- Reduced bandwidth requirement
- Reduced load on servers
- Access control and logging

Popular Proxy Caches

- Apache proxy
- MS proxy server
- WinProxy
- Squid
  - Squid is popular because it is powerful, configurable and free
- Many others

WEB SERVER

- Web server is a computer where the web content is stored
- Basically web server is used to host the web sites but there exists other web servers also such as gaming, storage, FTP, email etc.
- When client sends request for a web page, the web server search for the requested page if requested page is found then it will send it to client with an HTTP response.

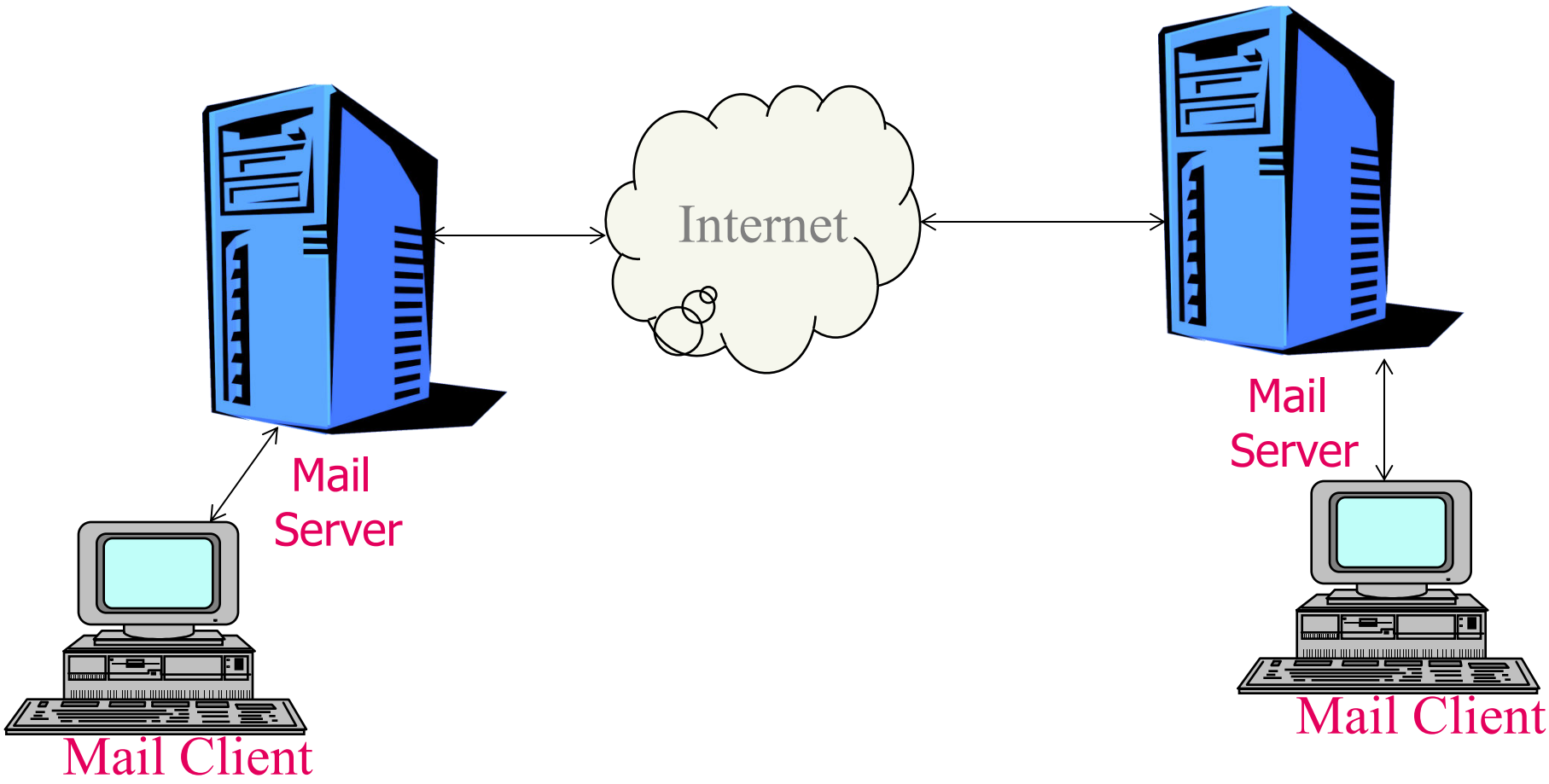
Web Server

- HTTP (Hyper Text Transfer Protocol) is used to transfer web pages from a Web Server to Web Client (Browser)
- Web Pages are arranged in a directory structure in the Web Server
- HTTP supports CGI (Common Gateway interface)
- HTTP supports Virtual Hosting (Hosting multiple sites on the same server)
- Popular Web Servers
  - Apache
  - Windows IIS
  - IBM Websphere

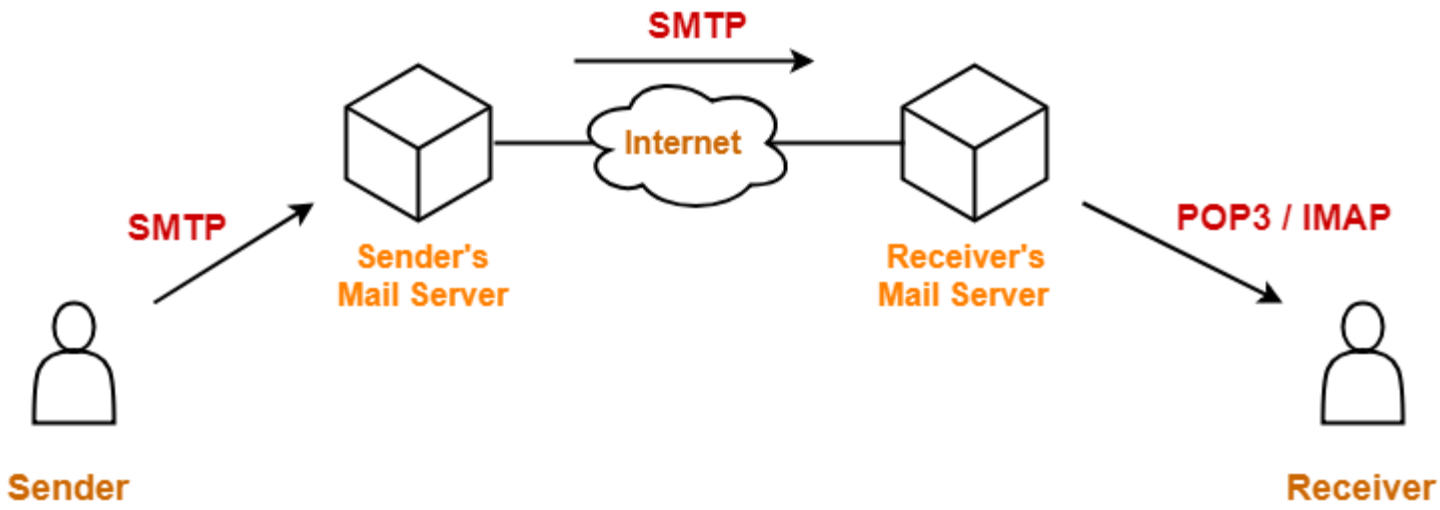
EMAIL

- SMTP is short for Simple Mail Transfer Protocol.
- It is an application layer protocol.
- It is used for sending the emails efficiently and reliably over the internet.

Mail Architecture



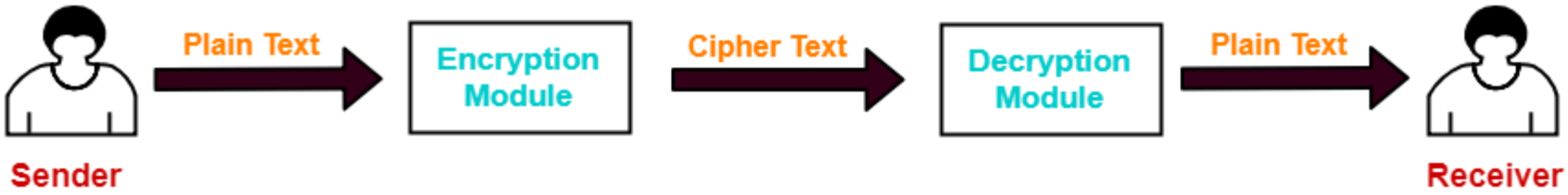
Mail Architecture



Network Security

Network Security

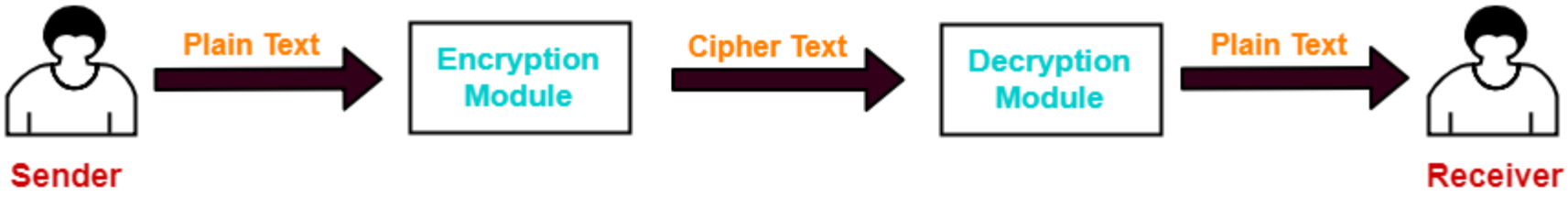
- Cryptography comes from Greek words for “secret writing”
- Cryptography is a method of storing and transmitting data in a particular form.
- It ensures that only the person for whom the message is intended can read the message.
- The message exchange using cryptography involves the following steps-



Cryptography

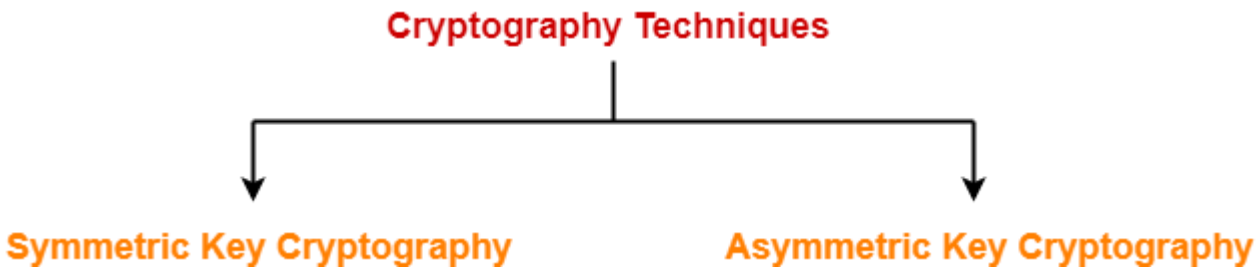
Network Security

- **At sender side,**
  - Using an encryption algorithm, the message is converted into an unreadable form.
  - The message in unreadable form is called as cipher text
- **At Receiver side,**
  - Using a decryption algorithm, the message is again converted into the readable form.
  - Then, receiver can read the message.



Cryptography Techniques-

- Cryptography techniques may be classified as-

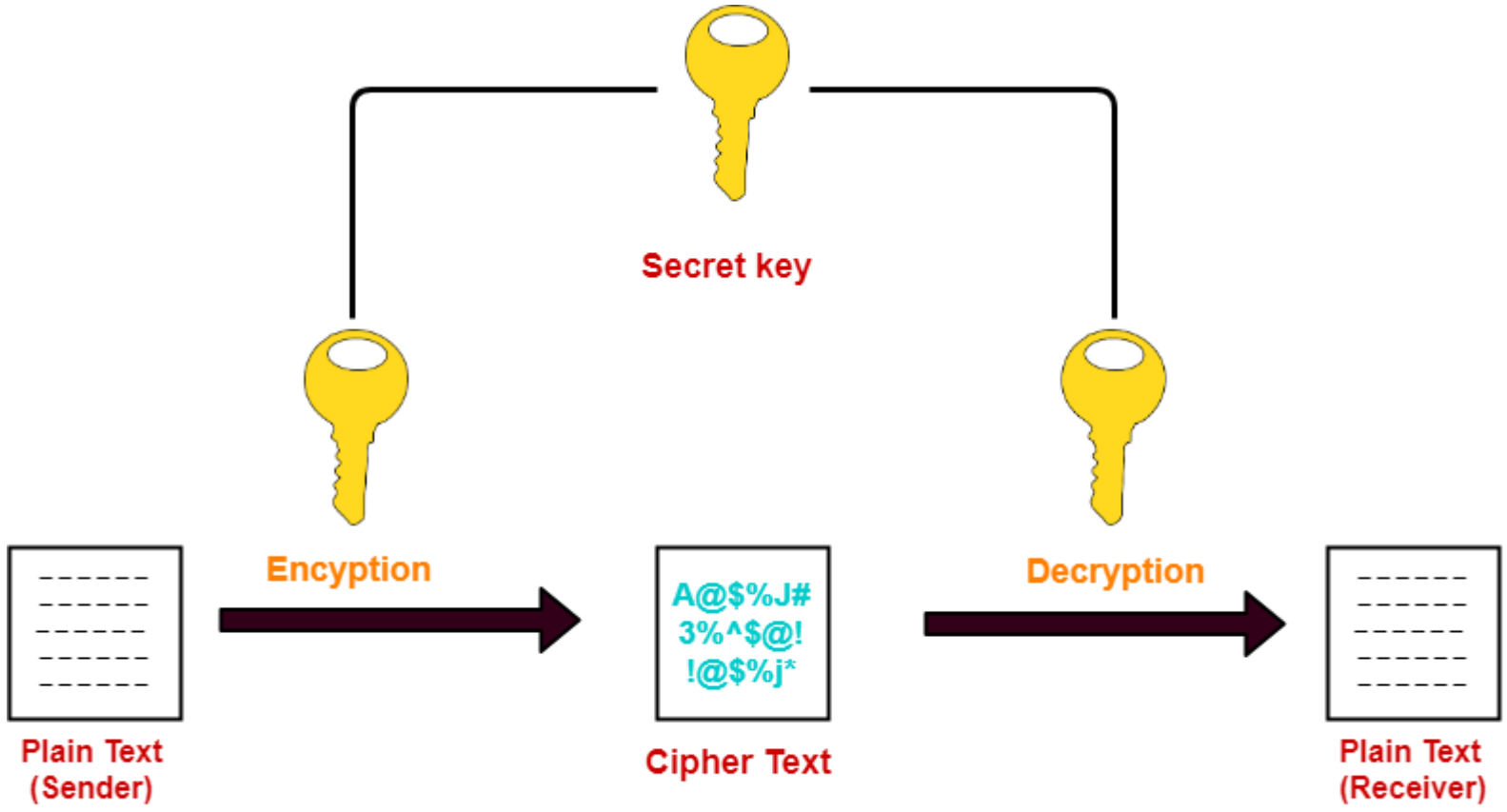


- **Symmetric Key Cryptography-**
  - Both sender and receiver uses a common key to encrypt and decrypt the message.
  - This secret key is known only to the sender and to the receiver.
  - It is also called as secret key cryptography.

Some of the encryption algorithms that use symmetric key are-

- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)

Symmetric Key Cryptography-



Symmetric Key Cryptography

Asymmetric Key Cryptography-

In this technique,

- Sender and receiver use different keys to encrypt and decrypt the message.
- It is called so because sender and receiver use different keys.
- It is also called as public key cryptography.

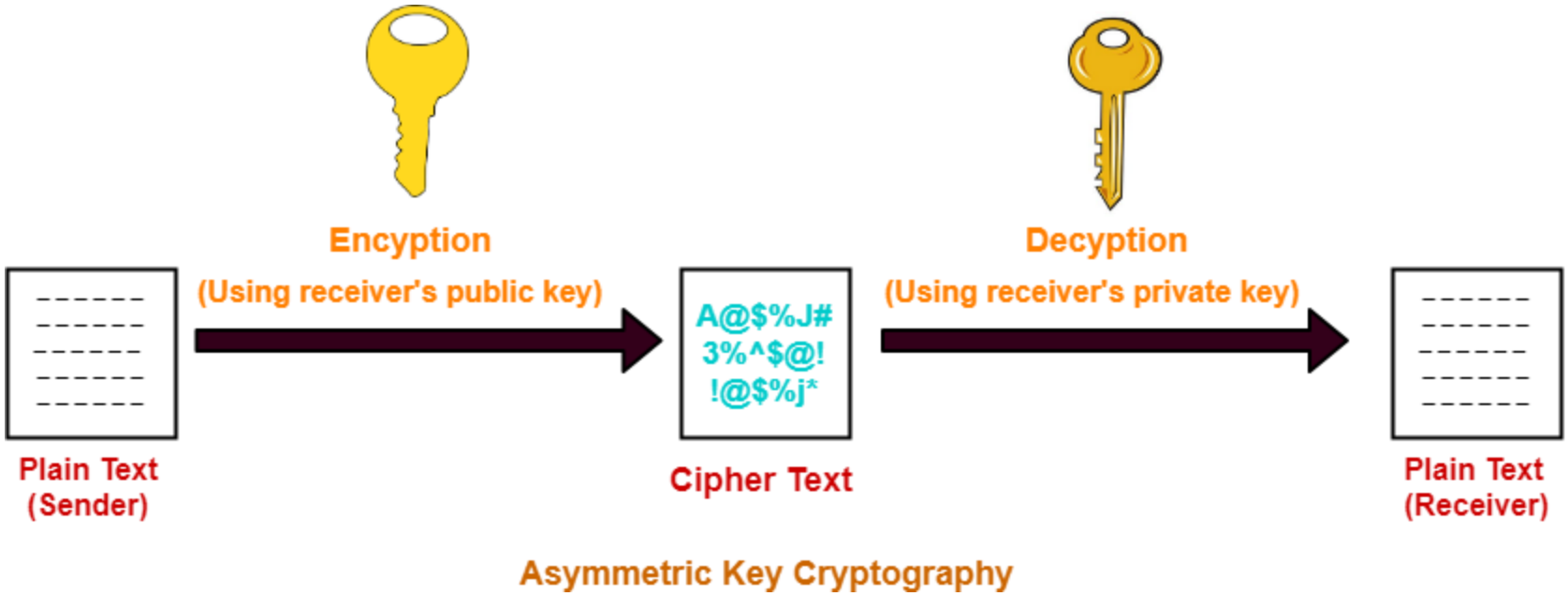
At sender side,

- ✓ Sender encrypts the message using receiver's public key.
- ✓ The public key of receiver is publicly available and known to everyone.
- ✓ Encryption converts the message into a cipher text.
- ✓ This cipher text can be decrypted only using the receiver's private key.

At receiver side,

- ✓ Receiver decrypts the cipher text using his private key.
- ✓ The private key of the receiver is known only to the receiver.
- ✓ Using the public key, it is not possible for anyone to determine the receiver's private key.
- ✓ After decryption, cipher text converts back into a readable format.

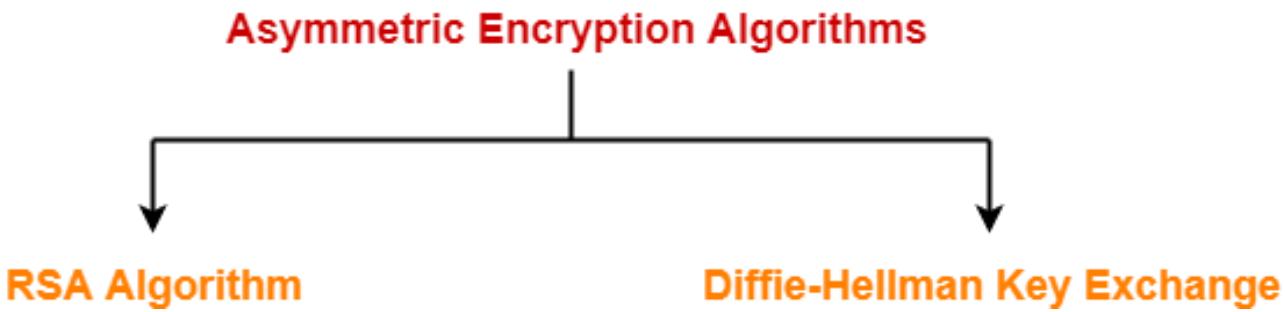
Asymmetric Key Cryptography-



Asymmetric Key Cryptography

Asymmetric Encryption Algorithms-

The famous asymmetric encryption algorithms are-



- RSA Algorithm
- Diffie-Hellman Key Exchange