Application Layer and Security

CHAPTER 8

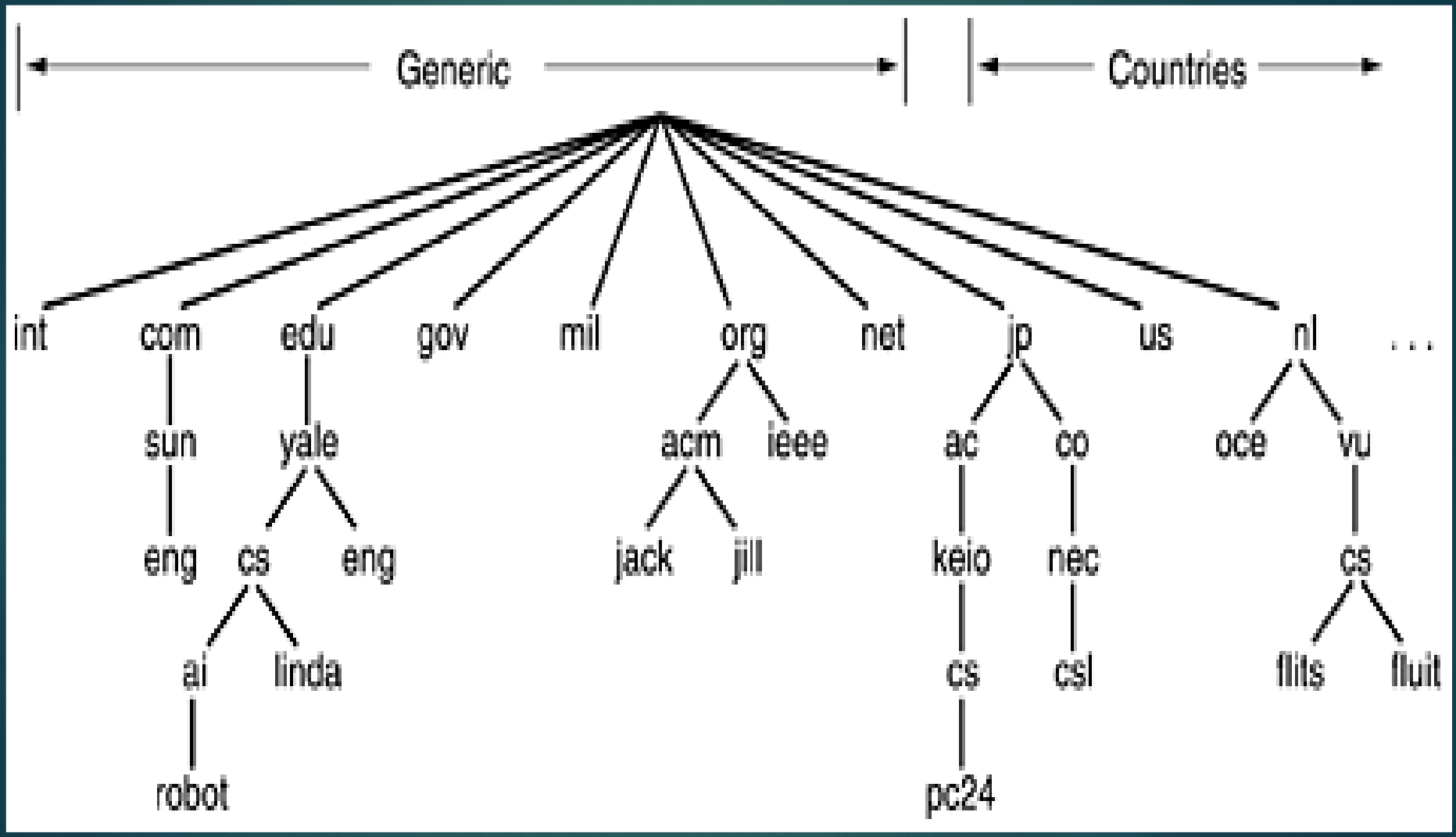
Domain Name System

- The IP addresses are not easy to remember
- ASCII equivalent names for the computers should be assigned, which are easy to remember
- Networks do not understand ASCII strings
- A mechanism that converts the ASCII string to the IP and vice versa is called DNS or Domain Name System

DNS

- To map a name onto an IP address, an application program calls a library procedure called the **resolver**
- The resolver sends a UDP packet to a local DNS server, which then looks up the name and returns the IP address to the resolver, which then returns it to the caller
- After finding the IP address, the program can then establish a TCP connection with the destination or send it UDP packets

DNS Name Space



DNS (Cont…)

- Domain name starts with sub domain then next level and then final domain
- Domain names are case insensitive
- Component name can be 63 character long while the full name cannot exceed 255 character
- Every domain, whether it is a single host or a top-level domain, can have a set of **resource records** associated with it. When a resolver gives a domain name to DNS, what it gets back are the resource records associated with that name

Resource Records

Domain_name Time_to_live Class Type Value

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

Resource Records

```
; Authoritative data for cs.vu.nl
cs.vu.nl.        86400   IN  SOA     star boss (9527,7200,7200,241920,86400)
cs.vu.nl.        86400   IN  TXT     "Divisie Wiskunde en Informatica."
cs.vu.nl.        86400   IN  TXT     "Vrije Universiteit Amsterdam."
cs.vu.nl.        86400   IN  MX      1 zephyr.cs.vu.nl.
cs.vu.nl.        86400   IN  MX      2 top.cs.vu.nl.

flits.cs.vu.nl.  86400   IN  HINFO   Sun Unix
flits.cs.vu.nl.  86400   IN  A       130.37.16.112
flits.cs.vu.nl.  86400   IN  A       192.31.231.165
flits.cs.vu.nl.  86400   IN  MX      1 flits.cs.vu.nl.
flits.cs.vu.nl.  86400   IN  MX      2 zephyr.cs.vu.nl.
flits.cs.vu.nl.  86400   IN  MX      3 top.cs.vu.nl.
www.cs.vu.nl.    86400   IN  CNAME   star.cs.vu.nl
ftp.cs.vu.nl.    86400   IN  CNAME   zephyr.cs.vu.nl
```

E-mail Architecture and Services

- Consist of two subsystems: **user agents**, which allow people to read and send e-mail, and the **message transfer agents**, which move the messages from the source to the destination
- The user agents are local programs that provide a command-based, menu-based, or graphical method for interacting with the e-mail system
- The message transfer agents are typically system **daemons**, that is, processes that run in the background. Their job is to move e-mail through the system.

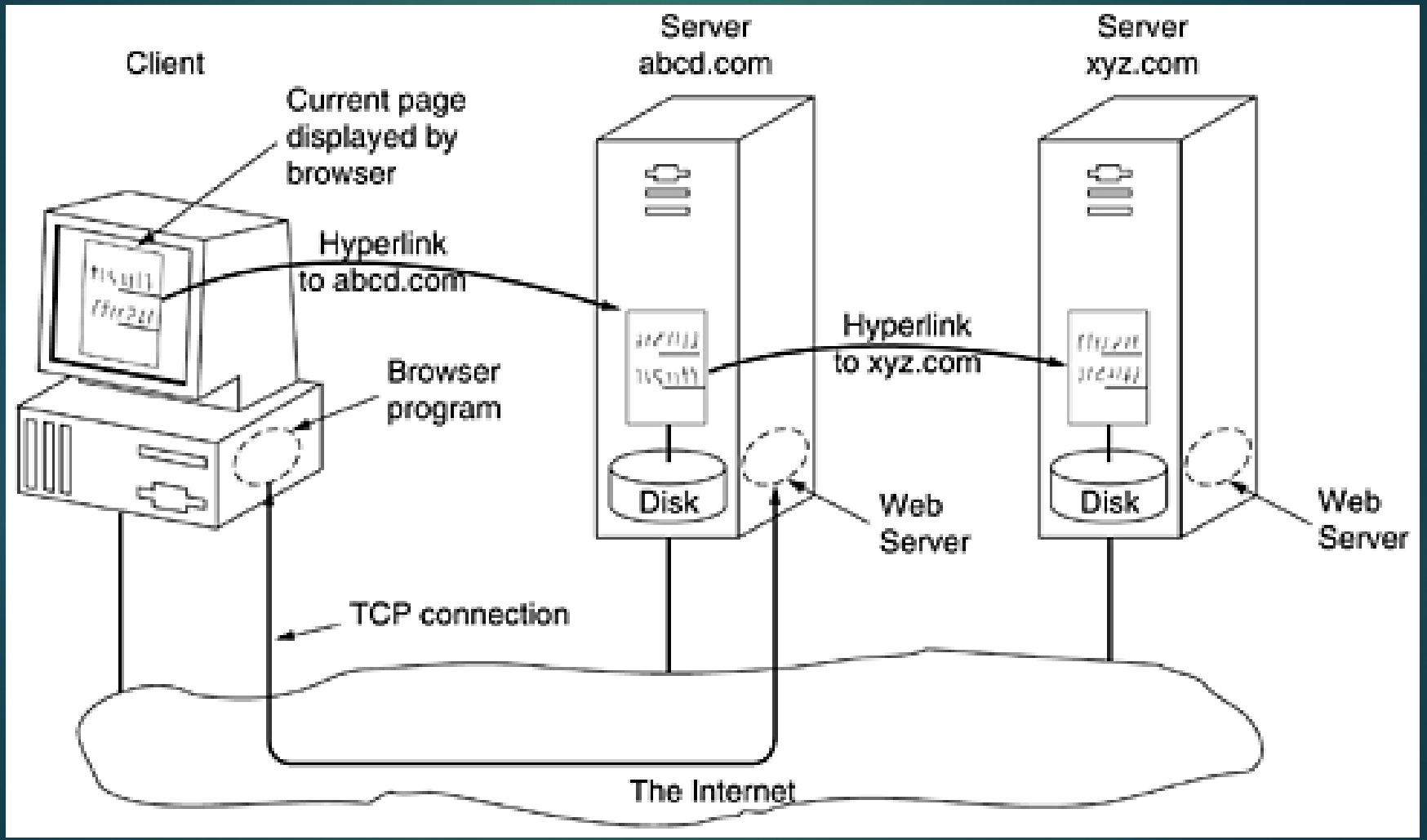
Functions of E – mail System

- **Composition:** refers to the process of creating messages and answers. For example, when answering a message, the e-mail system can extract the originator's address from the incoming e-mail and automatically insert it into the proper place in the reply.
- **Transfer:** refers to moving messages from the originator to the recipient. This requires establishing a connection to the destination or some intermediate machine, outputting the message, and releasing the connection. The e-mail system should do this automatically, without bothering the user.

Functions of E – mail System

- **Reporting:** has to do with telling the originator what happened to the message.
- **Displaying:** Proper formatting or conversion of files needed to make the massage understandable.
- **Disposition:** is the final step and concerns what the recipient does with the message after receiving it. Possibilities include throwing it away before reading, throwing it away after reading, saving it, and so on. It should also be possible to retrieve and reread saved messages, forward them, or process them in other ways.

World Wide Web



WWW steps - Client

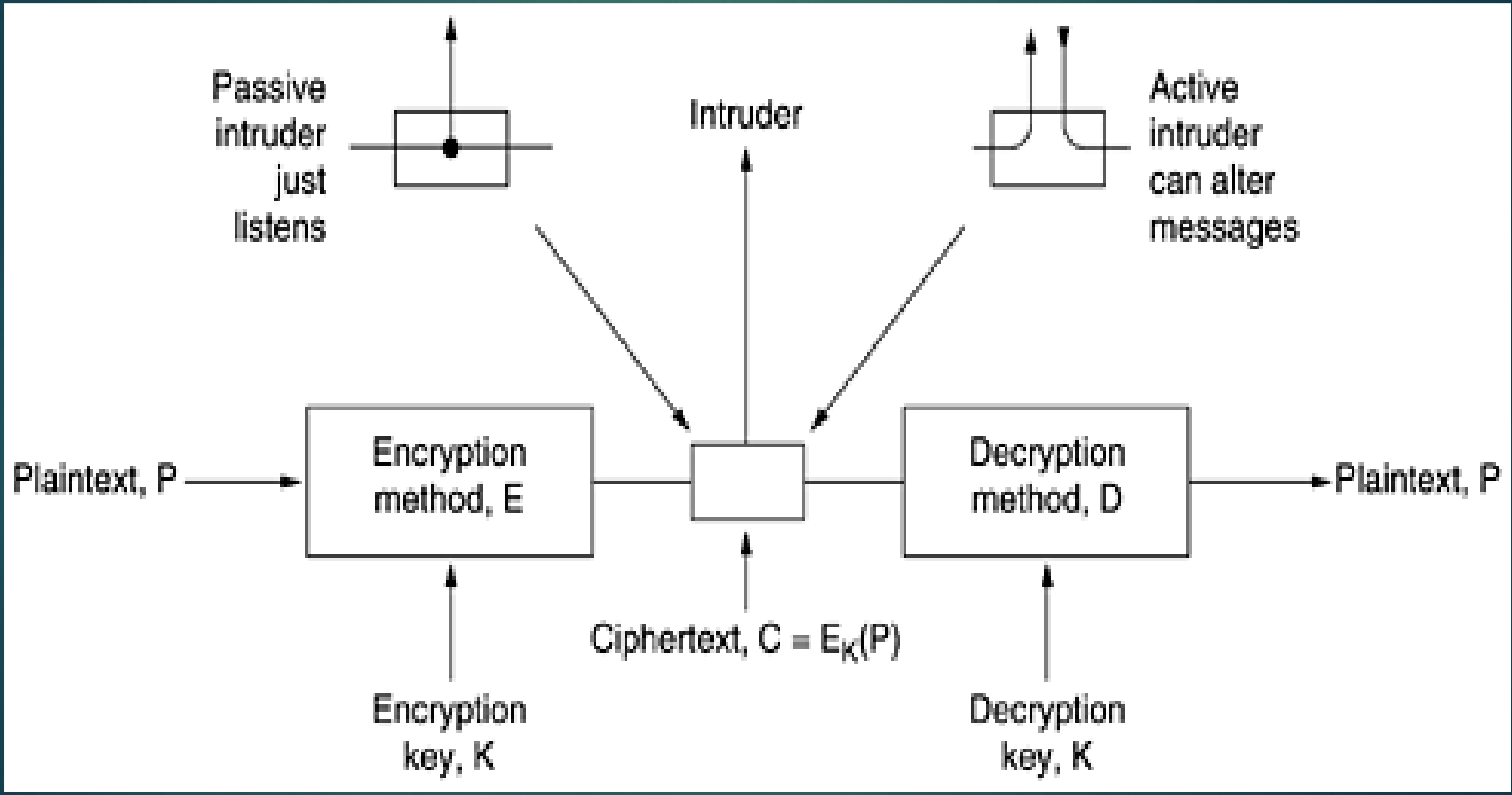
- The browser determines the URL (by seeing what was selected).
- The browser asks DNS for the IP address of *www.itu.org*.
- DNS replies with 156.106.192.32.
- The browser makes a TCP connection to port 80 on 156.106.192.32.
- It then sends over a request asking for file */home/index.html*.
- The *www.itu.org* server sends the file */home/index.html*.
- The TCP connection is released.
- The browser displays all the text in */home/index.html*.
- The browser fetches and displays all images in this file.

WWW Steps - Server

- Accept a TCP connection from a client (a browser).
- Get the name of the file requested.
- Get the file (from disk).
- Return the file to the client.
- Release the TCP connection.

Network Security

Cryptography



Cryptography Algorithms

- Private Key
- Public Key
- Symmetric Key
- Asymmetric Key

Substitution Cyphers

plaintext: a b c d e f g h i j k l m n o p q r s t u v w x y z

ciphertext: Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

Transposition Cyphers

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB