COMPUTER NETWORK

Page No.
Date

Unit-5 Application Layer

ONE SHOT + 3 PYQ SOLUTIONS

Topics :-

1. Application layer & its functions.
2. WWW
3. * DNS [2021-22, 22-23, 18-19]
4. HTTP [2018-19]
5. * FTP [2021-22, 22-23]
6. Remote Login Protocol
   TELNET & SSH [2018-19]
7. * Network Management [SNMP] - [2022-23, 18-19]
8. * EMAIL protocol [SNMP, POP3, IMAP]
   → [2021-22, 18-19, 22-23]
9. Data Compression & its Types
10. Cryptography & its Types

* → RSA Algo. with example - [2022-23]

Page No.:
Date:

[AKTU- 2021-22]

* Application Layer

→ It is the top most layer in both the the OSI and TCP/IP models.
→ It provides the interface b/w the application software on a device and the underlying network protocols.
→ It delivers the standard interface that applications can use transmit and obtain info. to communicate with each other over the network.

Functions

→ It determines the comm^n patner to whom data will be transmitted.
→ Spefiy the availability of resources.
→ Interface b/w user applications and the network.
→ This layer provides email services.
→ provides file transfer access and management.

Protocols of the Application layer in OSI model:

1. SMTP - Simple Mail Transfer Protocol
2. HTTP - Hypertext Transfer Protocol
3. FTP - File Transfer Protocol
4. DNS - Domain Name System
5. SNMP - Simple Network management Protocol.
6. TELNET - Telecommunication network.

Multi Atoms

Page No.
Date / /

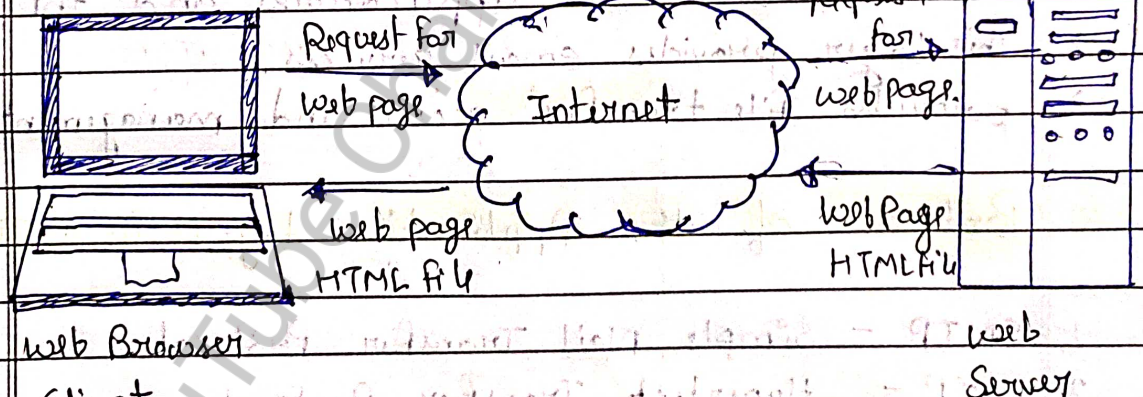
* World Wide Web

→ www, often simply referred to as "the web" is a vast information system, where documents and other web resources are identified by URL (Uniform Resource Locators) and can be accessed via the Internet.

→ invented by Sir Tim Berners-lee in 1989.

Key Components of the www:

1. (Web Pages) 2. (Web Browser) 3. (web Servers)
4. (URL) 5. (HTTP / HTTPS)



Page No.:
Date:

[AKTU-2021-22, 2022-23, 2018-19]

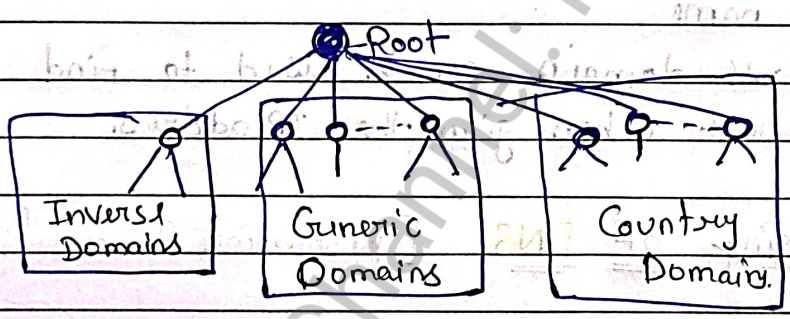
* Domain Name System [DNS]

→ As we know human beings are not comfortable in remembering numbers so to remember IP address of a website or mail account in Internet is difficult.

→ Domain Name System solve this problem. DNS can map a name to an address and conversely an address to a name.

→ However, for a person it is convenient to use names instead of addresses.

→ In the Internet, the domain name space is divided into three sections.



A. Generic Domains

→ In generic domain the registered hosts are define according to their generic behaviours. They are not restricted by country or region.

1) aero - Airlines
2) biz - business
3) com - Commercial
4) coop - Cooperative
5) edu - Education
6) gov - Government
7) info → Info. service
8) int - International org.
9) mil - Military
10) museum - Museums
11) name - personal names
12) net - Network Centers
13) org - Non profit Org.
14) pro - professional org.

Multi Atoms

Page No.
Date: / /

B. Country domains :

→ Country domains are two letters designated for specific country or territory, based on country code.

ex = .us - united state
.in - india. (academic institutes in india use .ac.in - gkte.ac.in)

C. Inverse domains

→ The inverse domain is used for mapping an address to a name

→ inverse domain can be used to find the name of a host when given the IP address.

Working of DNS [Resolution Process]

→ To map an address to a name or a name to an address we use a DNS client known as resolver.

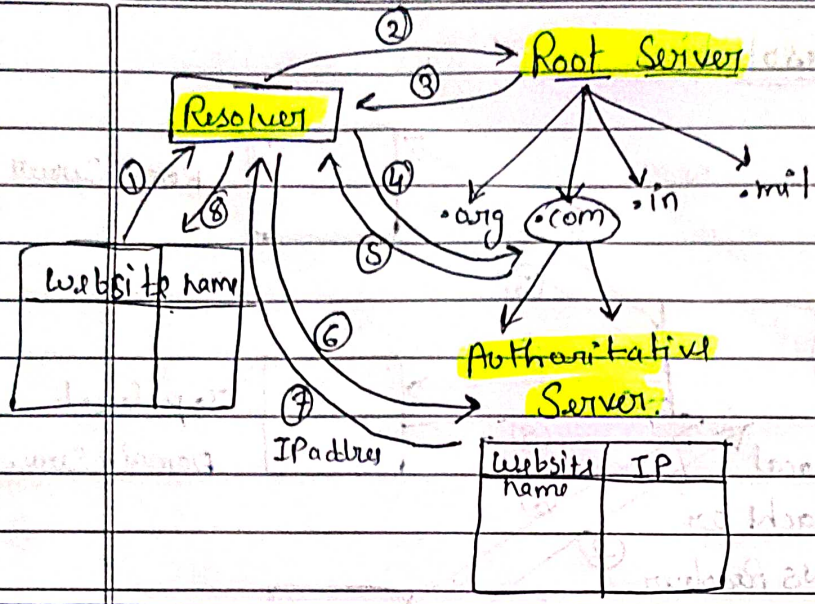
→ The resolver approaches the nearest DNS server with a mapping request.

→ If the server has the info. it provides the resolver with the info.

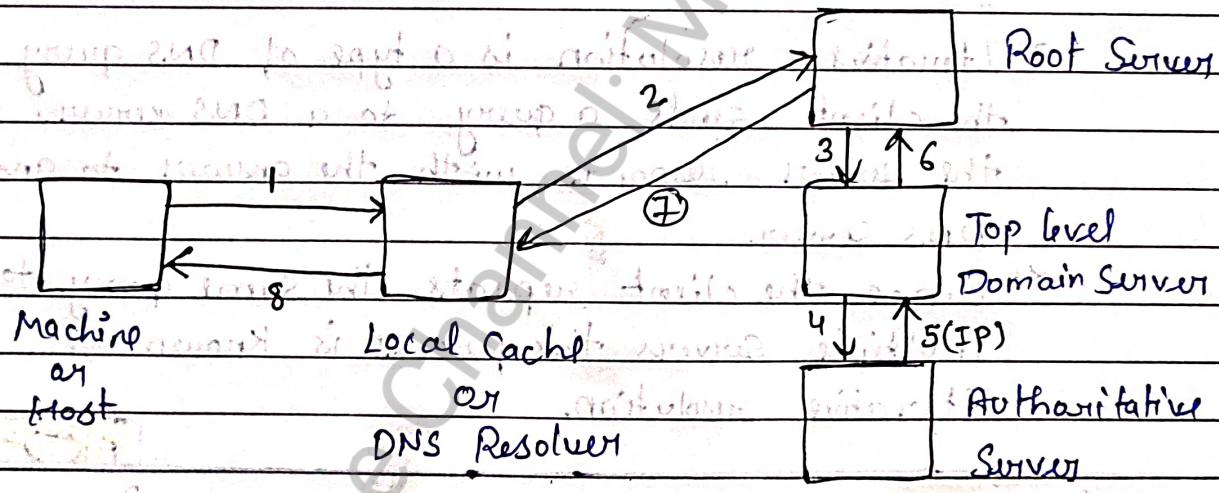
→ After the resolver receives the mapping it interprets the response and delivers the result to the process that requested it.

→ Resolution can be either recursive or iterative.

Page No.:
Date:



A). Recursive Resolution



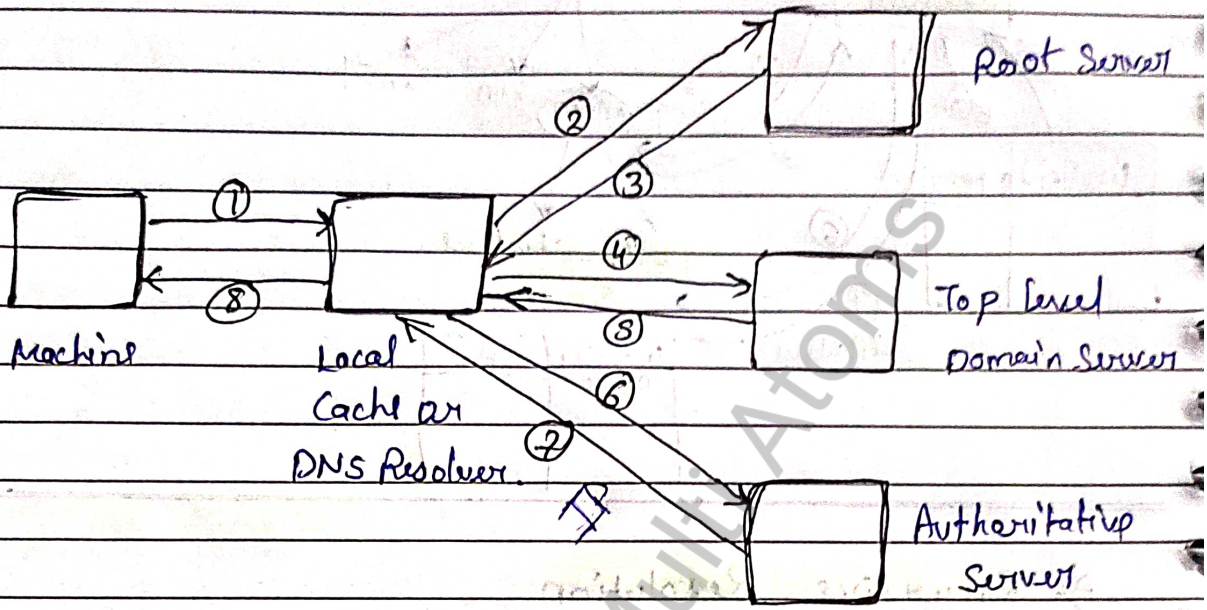
→ First Host check the IP address into Local cache if there is IP found then it responds otherwise it move to root Server.

→ It send query to Top level server and Authoritative Server send IP address to Root Server.

→ Now, query is finally resolved, the response travel back to the requesting client.

Page No.
Date / /

B. **Iterative Resolution**



→ Iterative resolution is a type of DNS query where the client sends a query to a DNS server, and the server responds with the answer to another DNS server.

→ Since the client repeats the same query to multiple servers this process is known as Iterative resolution.

AKTU-2018-19

* **HTTP** (Hyper Text Transfer Protocol)

→ It is a protocol used to access the data on the world wide web (www).

→ Port No. 80.

→ Uses TCP to achieve reliability.

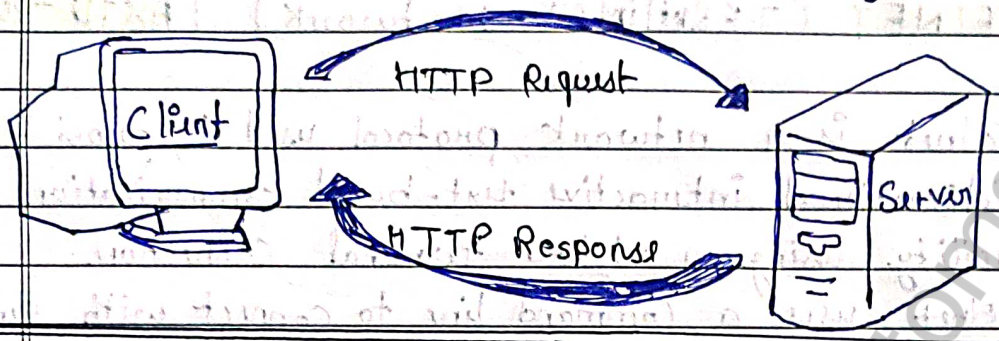
→ Stateless ⇒ It is a stateless protocol. Client & Server know each other only during the current request.

→ Inband Protocol ⇒ generates commands & data from same port.

Multi Atoms

Page No.:
Date:

→ Http 1.0 - non-persistant connection (multiple connection)
→ Http 1.1 - persistant connection (single connection).

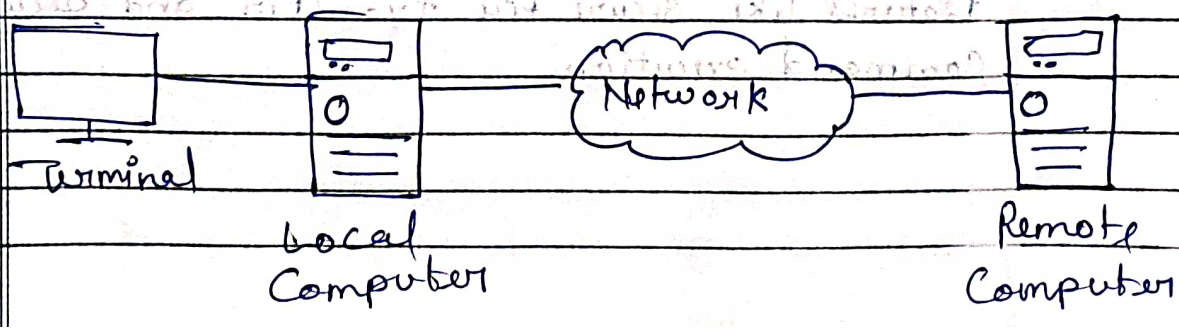


AKTU - 2021-22, 22-23

* **FTP** (File Transfer Protocol)
It is a standard network protocol used for transferring files between a client and a server on a computer network.
→ Reliable Protocol
→ Not Inband : (port no 20) for data and (21) for control commands like user identification, password.
→ Data connection is non-persistent.
→ Control connection is persistent.
→ Stateful (info about data) store.

* Remote Login Protocol

→ Remote Login Protocol, allowing users to access to a remote host/machine and use their terminals connected to the networks.



Multi Atoms

Page No.
Date / /

→ There are two protocols. (① TELNET ② SSH).

1. TELNET (TERMINAL Network) [AKTU - 2018-19]

→ Telnet is a network protocol used to provide a bidirectional interactive text-based communication facility using a virtual terminal connection.
→ Telnet uses a command line to connect with remote computer.
→ Client enters their username and password to access the remote computer.
→ It is not secure protocol because it is unencrypted.
→ Telnet transmits data, including usernames & passwords, in plaintext. This makes it highly vulnerable.
→ Due to its lack security features, Telnet has largely been replaced by more secure protocols for remote access like (SSH.)

2. SSH (Secure Shell).

→ Similar to telnet but it's provides encrypted communication over the network, offering a secure alternative to Telnet.
→ SSH uses port 22 by default and includes features like secure file transfer and secure command execution.

Multi Atoms

Page No.:
Date:

* Network Management

→ It means applications, tools and processes used to ensuring that network operates smoothly, securely and efficiently.

→ Main functions → operate, maintain, administer and secure network infrastructure.

1. SNMP [AKTU - 2022-23] [2018-19]

→ Simple Network Management Protocol is a widely used protocol for managing and monitoring devices on a network.

There are 3 components of SNMP:

i. SNMP Manager: A software system that collects and processes info. from network devices and monitor the network. → also known as Network Management Station (NMS)

2. SNMP agent: A software component that runs on network devices (such as routers, switches) and reports info. to the SNMP manager.

3. Management Information Base (MIB): A database or collection of info. that describes the structure of the network device data.
This info. is organized and stored hierarchically.

Page No.
Date / /

Email Protocols

→ Email protocols are rules and standards that governs the exchange of emails over the Internet.

→ They ensure that emails are sent, received and accessed efficiently and securely.

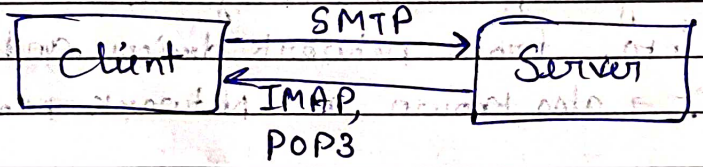
→ The primary email protocols are SMTP, IMAP & POP3.

3PYD [AKTU-2021-22]

1. **SMTP** (Simple Mail Transfer Protocol)

→ SMTP is used to send emails from client to a server or between server.

→ Companies use their SMTP server for marketing, password change and promotional emails



- Port 25 - Default (unencrypted port)
- Port 465 - Encrypted port.
- port 2525 - open at server side.

2. **MIME** (Multipurpose Internet Mail Extension)

→ It is able to send multiple attachments with a single message

→ Images, audio, video files etc.

Page No.:
Date:

→ MIME defines extensions to SMTP to support binary attachments.
→ Unlimited message length.

→ MIME Header → (MIME version, Content Type, Content-Type encoding, Content Id, Content discription).

2. Post Office Protocol 3 (POP3) Version 3.

→ POP3 is used to retrive emails from a server (single client).
→ It downloads emails from the server to the client divice.
→ Once downloaded, emails can be accessed offline.
→ Port 110 : Un-encrypted port.
→ Port 995 : encrypted port.

3. IMAP (Internet Passage Access Protocol).

→ IMAP versions (IMAP, IMAP2, IMAP3, IMAP4 etc).
→ retrive emails from multiple client.
→ have search option
→ It allows to access email without dowanloading them.
→ It allow multiple operations (create, delete, manpolate).
→ port 143 - Unencrypted port.
→ port 993 - Encrypted port.

Multi Atoms

Page No.
Date: / /

[AKTU - 2018-19]

Q. How is TFTP different from FTP?

→ Trivial file Transfer Protocol (TFTP) and file Transfer protocol (FTP) are both protocols used for transferring files b/w devices over a network but they have several key differences in terms of functionality and complexity.

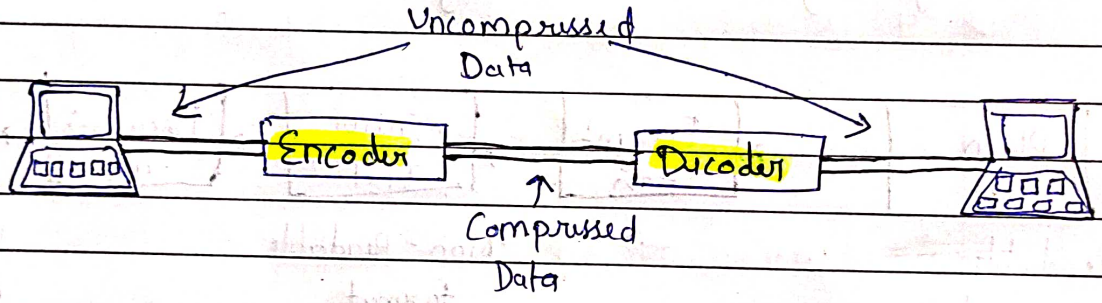
Feature	FTP	TFTP
protocol Type	TCP	UDP
Port no.	20, 21	69
Complexity	High	Low
Security	Basic	None
Authentication	Yes	No
Use Cases	Complex file management, websites.	Simple file transfers, read and write.
performance	Handles large files less fast.	fast, Handles simple file.

Multi Atoms

Page No.:
Date:

* Data Compression

→ It is the way of downloading the compressed form of text, audio and video data using the computer.
→ It is essential for efficient storage and transmission of different type of data.
→ A data compression system consists of an encoder & a decoder.
→ The encoder performs compression of the incoming data and decoder is used for decompression and reconstruction.



Types of compression :

1. **Lossless** Compression

→ In lossless comparession, the redundant information contained in the data is removed.
→ There is no loss of information.
→ has lower comparision ratio.

2. **Lossy** Compression

→ there is a loss of Information in a controlled manner.
→ not completely reversible
→ but has higher comparission.

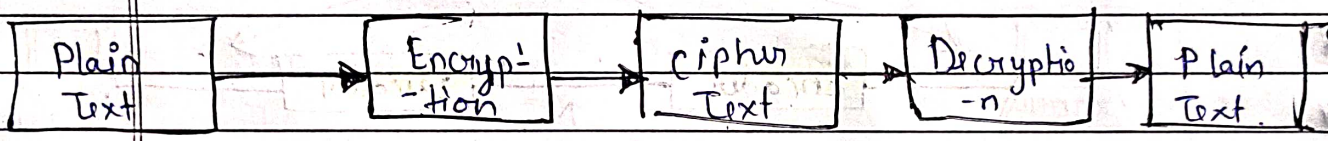
Multi Atoms

Page No.
Date / /

* Cryptography

→ It is a technique of securing communication by converting plain text into ciphertext. It involves various algorithms and protocols to ensure data confidentiality, integrity, authentication and non-repudiation.

→ "Crypt" means "hidden"
→ "graphy" means "writing"



Types of Cryptography

1. Symmetrical Encryption

→ This is the simplest kind of encryption that involves only one secret key to cipher and decipher information.

→ It uses a secret key that can either be a number, a word or a string of random letters. It is a blended with the plain text of a message to change the content in a particular way.

→ The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages.

Page No.:
Date:

→ The most popular Symmetric key cryptography systems are Data Encryption System (DES) and Advanced Encryption System (AES)

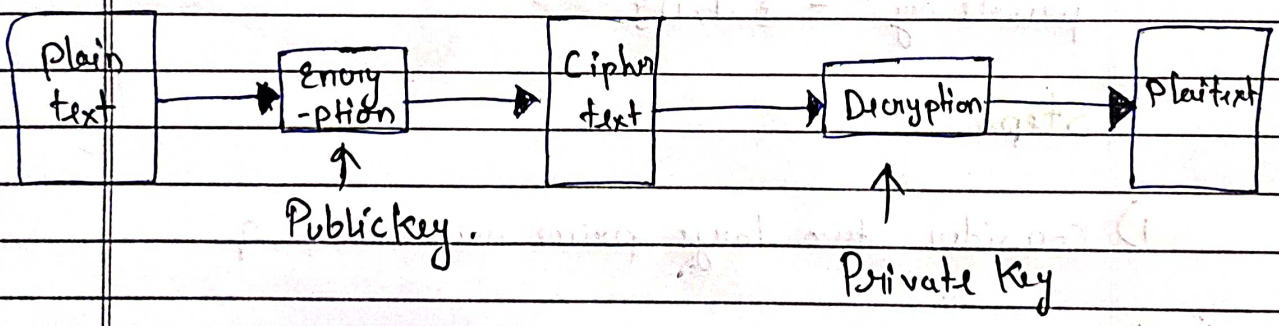
2. Asymmetric key Cryptography

→ A pair of keys is used to encrypt and decrypt info.

→ A receiver's public key is used for encryption and a receiver's private key is used for decryption.

→ You publish your public key to the world while keeping your private key secret.

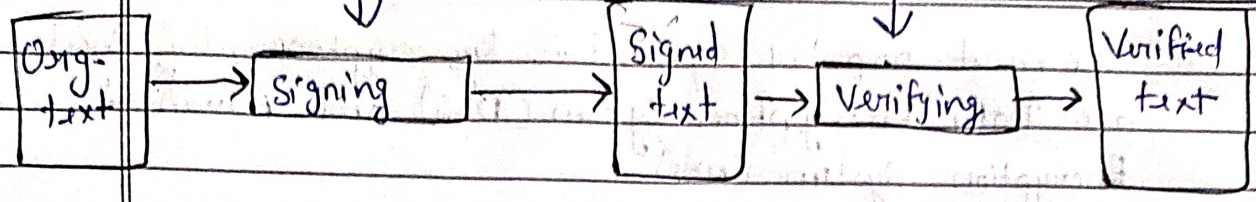
→ The most popular asymmetric key cryptography algorithm is the RSA algorithm. (Rivest - Shamir - Adleman)



3. Digital Signature

→ The signature is encrypted using the private key and decrypted with the public key.

→ More secure than handwritten signature.



[AKTU-2022-23]

* RSA Algorithm

→ RSA (Rivest - Shamir - Adleman) is an algorithm used to encrypt & decrypt messages.

⇒ It is an asymmetric cryptography algo.

Encryption – $C = P^e \bmod n$

Decryption – $P = C^d \bmod n$

public key = $\{e, n\}$
private key = $\{d, n\}$

Steps.

1) Consider two large prime numbers p, q.
2) Calculate $n = p \times q$
3) $\phi(n) = (p-1)(q-1)$ — $\phi(n)$ → Euler's function
4) choose a small number e, co-prime to $\phi(n)$
   $\gcd(e, \phi(n)) = 1$ & $1 < e < \phi(n)$
5) Find d, such that $d \times e \bmod \phi(n) = 1$

Page No.:
Date:

Example =

1) Two prime numbers $p = 3$, $q = 5$

2) $n = p \times q = 3 \times 5 = 15$ $\boxed{n = 15}$

3) $\phi(n) = (p-1)(q-1) = (3-1)(5-1) = 8$ $\boxed{\phi(n) = 8}$

4) Assume e such that $\gcd(e, \phi(n)) = 1$ &

$1 < e < \phi(n)$

$\boxed{e = 3}$

5) find d $\quad d \times e \bmod \phi(n) = 1$

$d \times 3 \bmod 8 = 1$

Let $d = 3$

$3 \times 3 \bmod 8 = 1$

$9 \bmod 8 = 1$

$\boxed{1 = 1}$

$\boxed{d = 3}$

1) public key = $\{e, n\} = \{3, 15\}$
2) private key = $\{d, n\} = \{3, 15\}$

Let Data (P) = 8 = plain text.

Encryption $C = P^e \bmod n = 8^3 \bmod 15 = 2$ $\boxed{C = 2}$

$(512 \bmod 15)$

Decryption $P = C^d \bmod n = 2^3 \bmod 15 = 8$ $\boxed{P = 8}$

$(8 \bmod 15)$