

Module 7 DNS

Saturday, 11 May 2024

7:34 PM

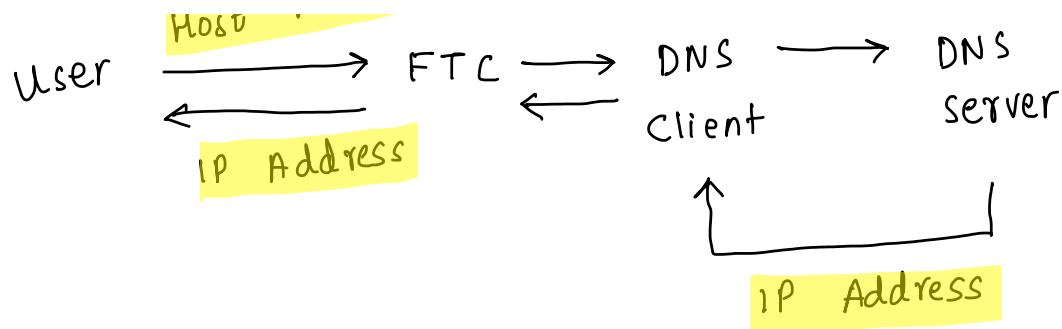
DNS:

- ★ It is a directory that can map name to IP Address.
- ★ The directory is distributed among many PCs.
- ★ In this method, the host that needs mapping can contact the closest computer holding the needed information.

Mapping of Name to Address:

- ★ User passes the host name to File Transfer Client.
- ★ Then File Transfer client passes host name to DNS Client.
- ★ DNS Client sends a message to DNS server with a query that gives file transfer server name using the known IP Addresses.
- ★ DNS server responds with File Transfer server IP Address.
- ★ DNS server passes the IP Address
- ★ The File Transfer client now uses the received IP Address to file transfer client.





Name Space :

- ★ Unique
- ★ Organized in 2 ways : Flat, Hierarchical

Flat Namespace :

- ★ Name assigned to address.
- ★ Sequence of character without structure.
- ★ Names may or may not have common section.
- ★ Dis. Adv : Can't be used in large system.

Hierarchical Name Space :

- ★ Name made of several parts.
- ★ First Part : Organization Nature
- ★ Second Part : Organization Name
- ★ Third Part : Department

Domain Name Space :

- ★ It was designed to have hierarchical namespace.

★ Inverted Tree Structure

★ Tree can only have 128 level.

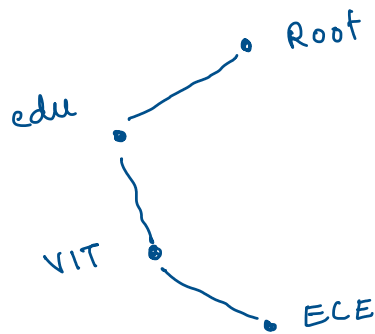
Label:

★ Each node in a tree has Label.

★ Maximum string length of 63 characters.

★ Root Label is empty string.

★ Children node should have different name.

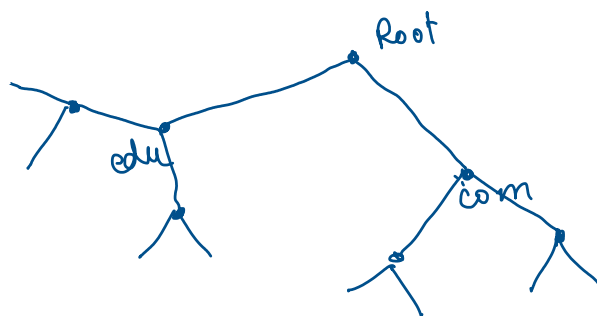


Domain Name:

★ Each node in a tree has domain name.

★ Separated by dots (.).

★ Read from node up to the root.



DNS in Internet:

★ Generic Domains E.g : edu, gov, info, org, ...

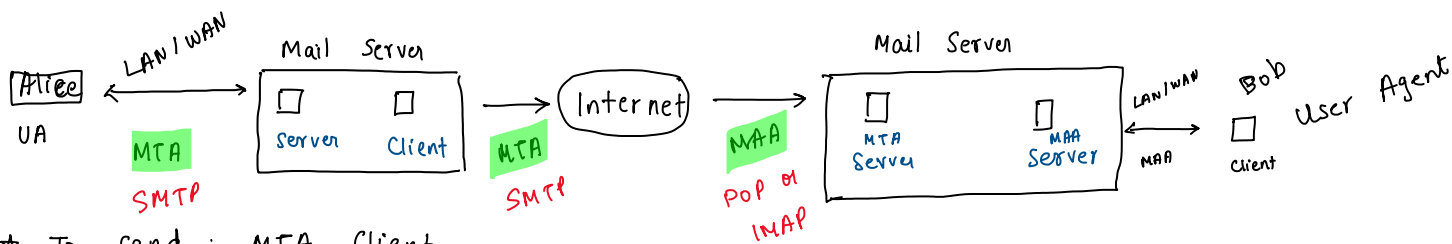
★ Country Domains E.g : in, us, au, ...

Module 7 SMTP

Sunday, 12 May 2024 8:17 AM

SMTP:

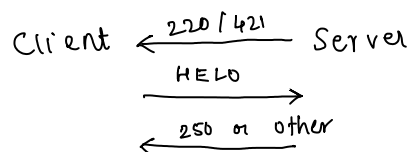
- ★ Components: User Agent, Message Transfer Agent, Message Access Agent.



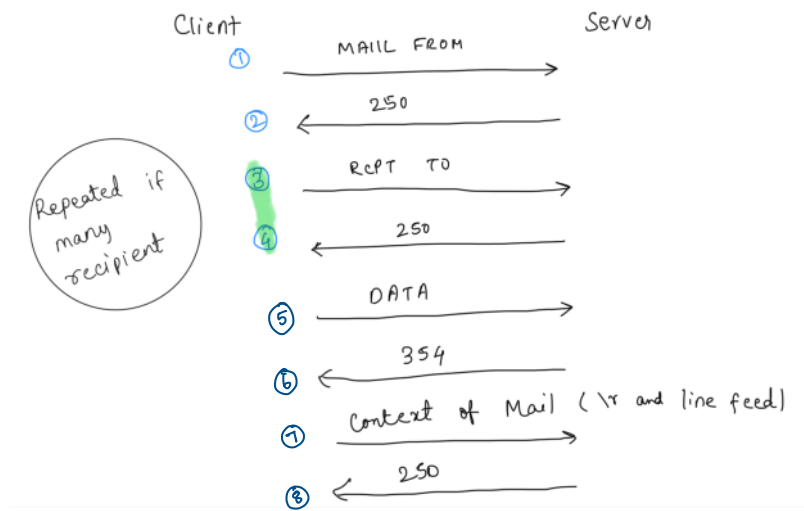
- ★ To send: MTA Client
- ★ To receive: MAA Server
- ★ SMTP is used 2 times, Sender to sender mail server and between two mail servers
- ★ SMTP uses commands and responses to transfer messages between Mail Server.
- ★ SMTP has 14 commands.
 - First 5 are mandatory
 - Next 3 is highly recommended.
 - Last 6 is seldom used

Mail Transfer Phases:

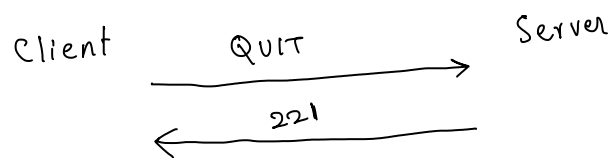
- ★ Connection Establishment
 1. server sends 220 to tell client that it is ready to receive mail. 421 - Service Not Available
 2. Client sends HELO message to identify using first name. It informs the domain name of client
 3. Server may responds with 250 - Request Command complete or something.



- ★ Mail Transfer



* Connection Termination.



Module 7 Cryptography

Sunday, 12 May 2024 9:15 AM

Given in Question

Additive Cipher = 15

hello

h - 7
e - 4
l - 11
l - 11
o - 14

Encryption

$$(7+15) \bmod 26$$

$$4+15 \bmod 26$$

$$11+15 \bmod 26$$

$$11+15 \bmod 26$$

$$14+15 \bmod 26$$

22 - w

19 - T

0 - A

0 - A

3 - D

Decrypt

w

22

$$(22-15) \bmod 26$$

7 - h

T

19

$$19-15 \bmod 26$$

4 - e

A

0

$$0-15 \bmod 26$$

11 - l

A

0

$$0-15 \bmod 26$$

11 - l

D

3

$$3-15$$

14 -

Negative
Add
+26
to that

RSA Cryptosystem:

Large Prime Number p and q

$$n = p \times q$$

$$\phi = (p-1) \times (q-1)$$

$$1 < e < \phi(n)$$

$$1 < e < \phi(n)$$

↓
coprime to $\phi(n)$

Encrypt the message: $C = (p^e) \bmod n$

Decrypt the message: $P = C^d \bmod n$

Example:

2 Prime Numbers
3, 5

$$n = 3 \times 5 = 15$$

$$\phi(n) = (3-1)(5-1) = 2 \times 4 = 8$$

$$(e \times d) \bmod \phi(n) = 1 ; \quad e \in (1, \phi(n))$$

Encryption:

$$(e \times d) \bmod 8 = 1 \quad e \times d = 9$$

Diff Combination: $1 \times 9, 9 \times 1, (3 \times 3)$

→ conditions for e

↑ condition satisfies

$$e = 3, d = 3$$

Encryption: $P = 8$ Given

$$C = p^e \bmod n = 8^3 \bmod 15$$

$$C = 512 \bmod 15$$

$$C = 2$$

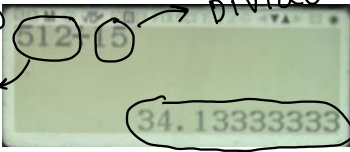
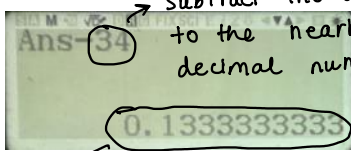
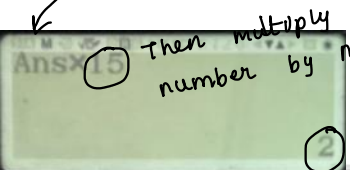
Decryption:

$$P = C^d \bmod n$$

$$= 2^3 \bmod 15$$

$$P = 8 \bmod 15 = 8$$

Mod Calculation
in Calculator:

- ①  Divide by n value
 8^3
- ②  Subtract the decimal to the nearby decimal number
- ③  Then multiply that number by n value
 → Final Answer

Example 2:

Two Prime Number: 7, 11

$$n = 7 \times 11 = 77$$

$$\phi(n) = (7-1)(11-1) = 60$$

$$(e \times d) \bmod n = 1$$

$$\text{---} \bmod 60 = 1$$

Given: $e = 13, d = 37$

$$C = p^e \bmod n = 5^{13} \bmod 77 = 26$$

Calculation:

$$5^{13} \div 77 = 15853287.34 \rightarrow \text{Multiply by 77} \rightarrow 26$$

$P = 26^{37} \bmod n$ = Fast Exponentiation Method is used

$$37 \rightarrow \text{Binary } 100101$$

Fast Exponentiation Method: Example

$$\begin{aligned} 13^{15} \bmod 60 &= (13^8 \cdot 13^4 \cdot 13^2 \cdot 13^1) \bmod 60 \\ 13^1 \bmod 60 &= 13 \\ 13^2 \bmod 60 &= (13 \cdot 13) \bmod 60 \\ (13 \bmod 60 \cdot 13 \bmod 60) \bmod 60 &= 49 \\ (13 \cdot 13) \bmod 60 &= 49 \\ 13^4 \bmod 60 &= (13^2 \cdot 13^2) \bmod 60 \\ (13^2 \bmod 60 \cdot 13^2 \bmod 60) \bmod 60 &= \end{aligned}$$

$$\begin{aligned}
 (49 \times 49) \bmod 60 &= 1 \quad \checkmark \\
 13^8 \bmod 60 &= (13^4 \cdot 13^4) \bmod 60 \\
 (13^4 \bmod 60 \times 13^4 \bmod 60) \bmod 60 \\
 (1 \cdot 1) \bmod 60 &= \underline{1} \quad \checkmark \\
 (13^8 \cdot 13^4 \cdot 13^2 \cdot 13^1) \bmod 60 \\
 (13^8 \bmod 60 \times 13^4 \bmod 60 \times 13^2 \bmod 60 \times 13^1 \bmod 60) \bmod 60 \\
 (1 \times 1 \times 49 \times 13) \bmod 60 \\
 &= 39 // = .
 \end{aligned}$$

Homework:

$$\begin{aligned}
 (e \times 37) \bmod 60 &= 1 \\
 e \cdot 37^{-1} \bmod 60 \\
 37^{q(60)-1} \bmod 60 &= 37^{15} \bmod 60 \rightarrow 13 \\
 C = P^e \bmod n &= 5^{13} \bmod 7 \cdot 7 = (20) \\
 P = x^{37} \bmod 7 \cdot 7 &= \underline{5}
 \end{aligned}$$