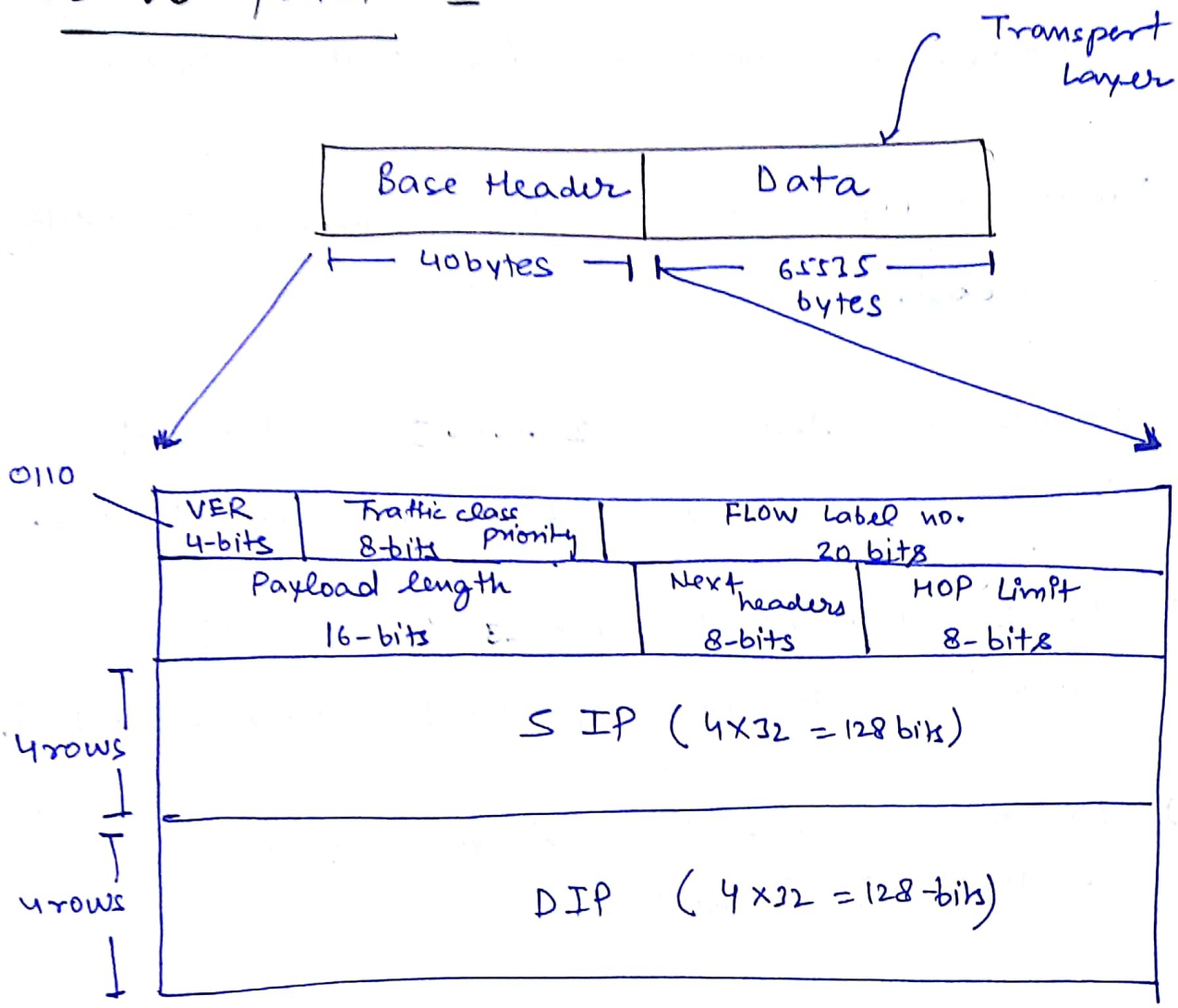
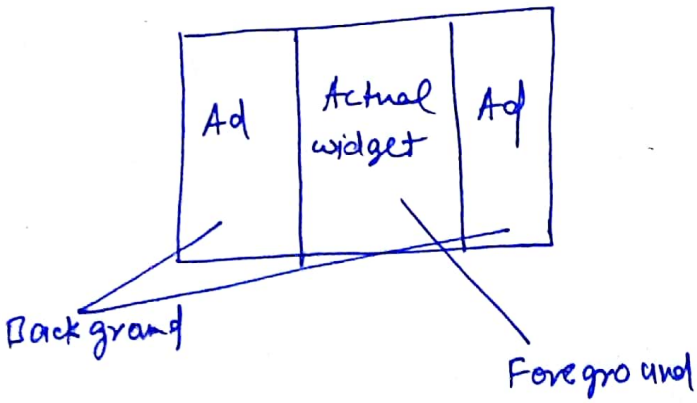
IPv6 packet –



- FTP is having high priority then SMTP.
- Foreground packets are having high priority than Background packets.

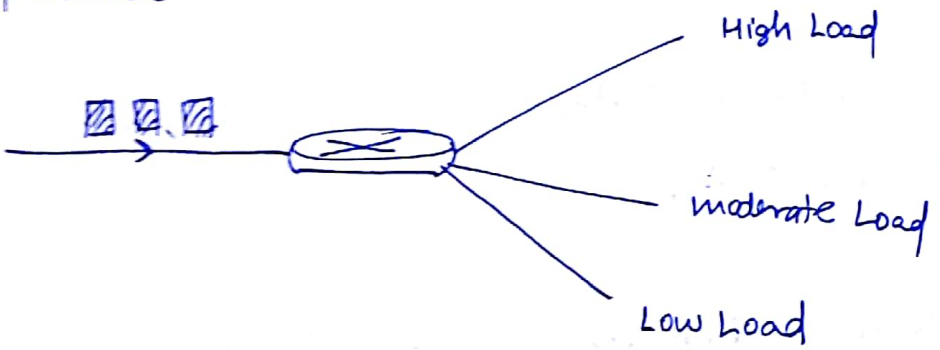


- Out of all packets, control packets have high priority.

- In case of IPv6 whenever a packet comes to the router different Loads of the network is given by RSVP and RTP.

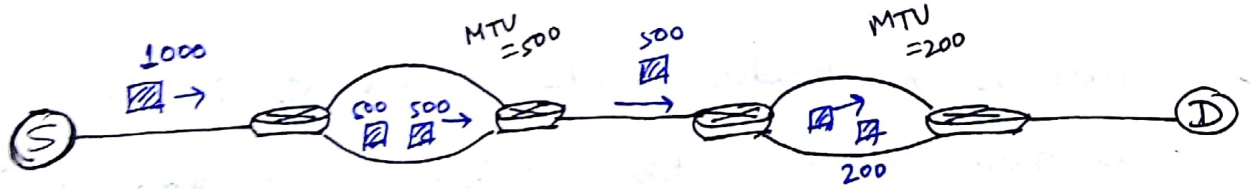
RSVP → Resource Reservation protocol

RTP → Real time protocol

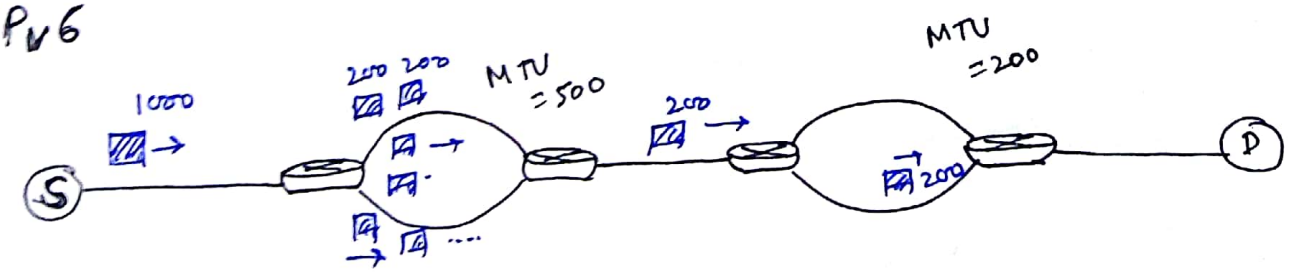


- The priority of a packet can be uniquely distinguished by (traffic class + flow label number).

IPv4



IPv6



MTU = min (MTU$_1$, MTU$_2$, ... MTU$_n$)

so, MTU = min(500, 200) = 200

- In IPv6 a packet is fragmented only at the starting router & defragmentation is done at destination router.

- Fragmentation is not compulsory that's why Fragmentation offset is provided in option field.

- Payload length indicates size of data, not whole packet like IPv4.

- Next header indicates if any headers are added along with the base header.

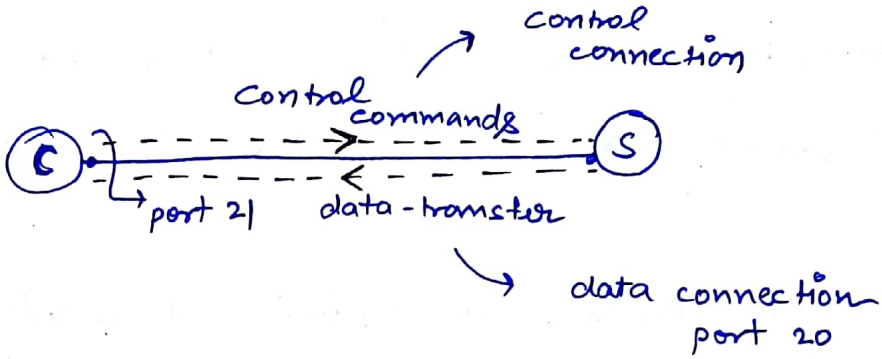
- Hop-limit is used to identify if any loop exist for the packet.

Drawback :-

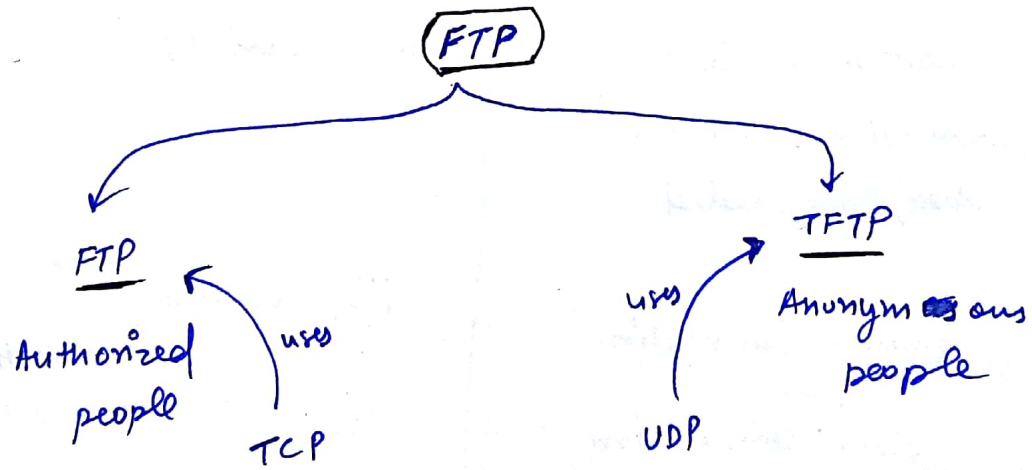
- There is no header checksum presents in IPv6 header as there are no better checksum algo available for IPv6 packet.

File transfer Protocol :-

- downloading a file
- client - server protocol



- FTP will send control commands on port 21 via a control connection.
- Once the File is about to download a seperate data connection is established on port 20.
- Once the file is completly downloaded data connection is closed but control connection will exist to download some files.

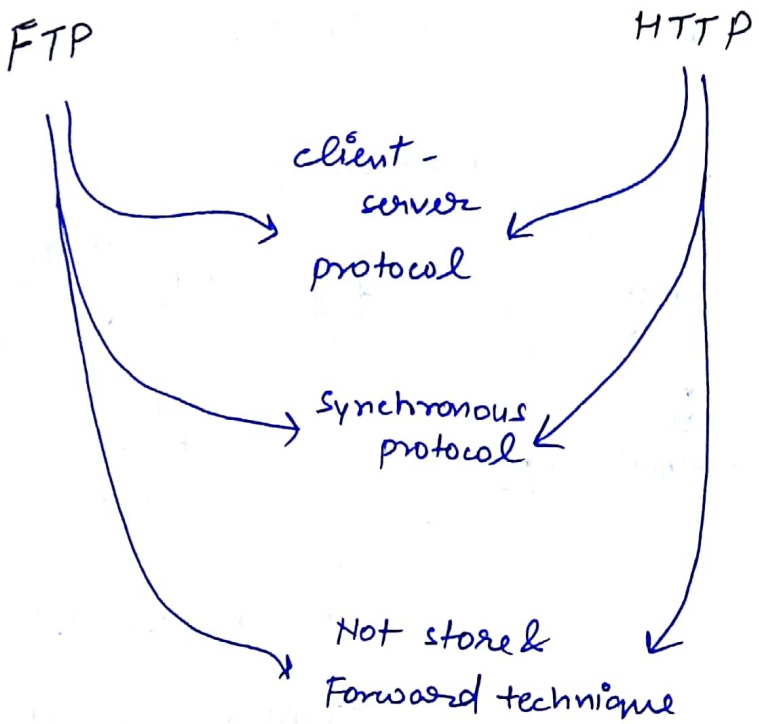


- In FTP version authorization and security is madatory so they use login credentials and paid for Net acess and downloading files.
Since they needs end-to-end connection before sending so they use TCP at transport layer, it also provide flow control.

- In TFTP version authorization and security is not necessary and no end-to end connection is needed so UDP is used.

FTP vs Telnet :-

FTP	Telnet
(i) downladding a large file	(i) chat operation (exchange of words)
(ii) port 20,21 as two connection (controll data) are needed	(ii) port 23
(iii) control connection & data connection	(iii) common connection



(i) control connection

(ii) Data connection

(i) persistent connection

(ii) Non - persistent connection

SMTP (simple Mail Transfer protocol) :-

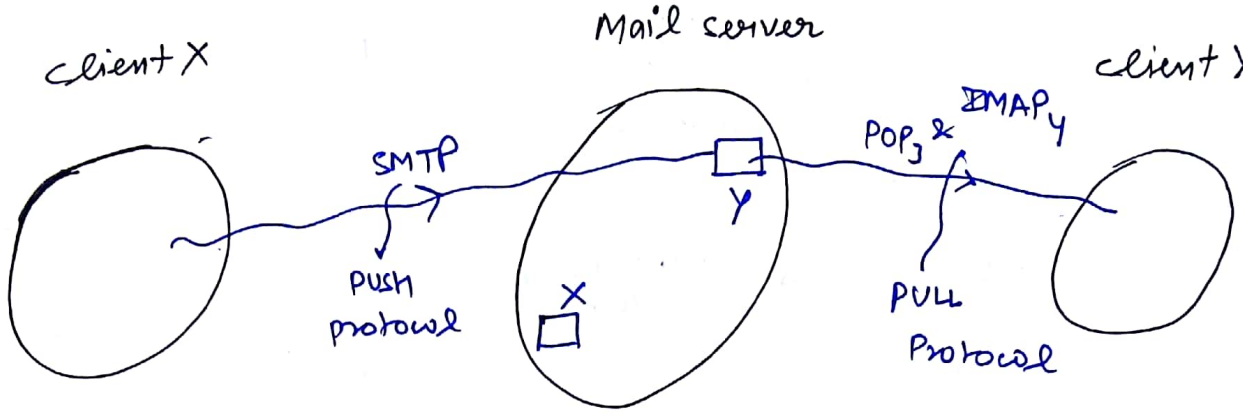
- text based protocol

MIME ⇒ (Multimedia Internet mail extension)

It is a text based protocol but we can send graphical data with the help of MIME which is provided by internet browsers.

- Port no : 25

- Uses Tcp at transport Layer.



POP → post office protocol

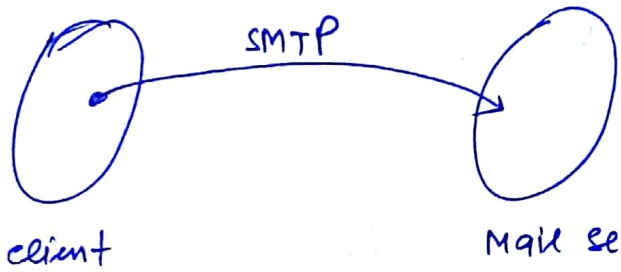
IMAP → Internet mail access protocol

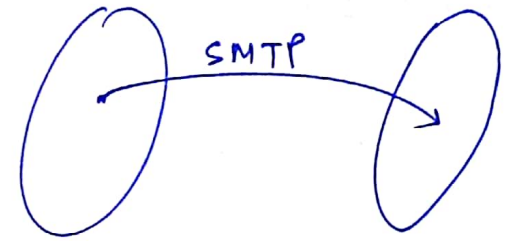
- "SMTP" is a PUSH protocol because it is used for sending mail to the mail server.

- POP_3 & $IMAP_4$ are PULL protocol because they are used for retriving the mails from the mail server.

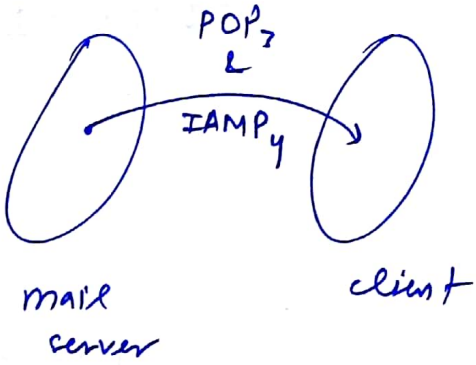
- SMTP combined with POP_3 & $IMAP_4$ is a client-to-client protocol with a mediation done by mail server.

- SMTP is a store and forward protocol because the mail is stored on mail server then are forwarded to other client.





eg: gmail



eg: hotmail

- SMTP used "base 64 encoding" i.e whole data (binary of mail is encoded to base 64 value to provide security.

Base 64 encoding:-

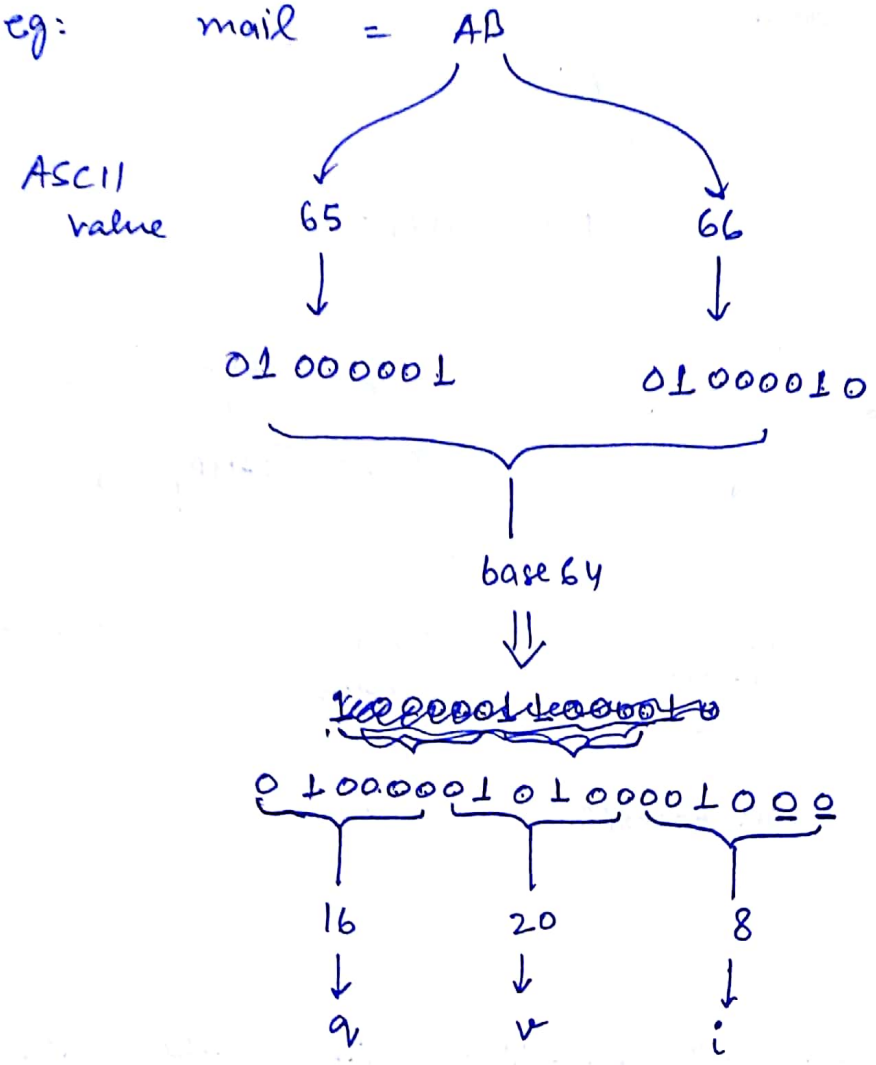
[a-z] → 0-25

[A-Z] → 26-51

[0-9] → 52-61

+ / → 62, 63

eg: mail = AB

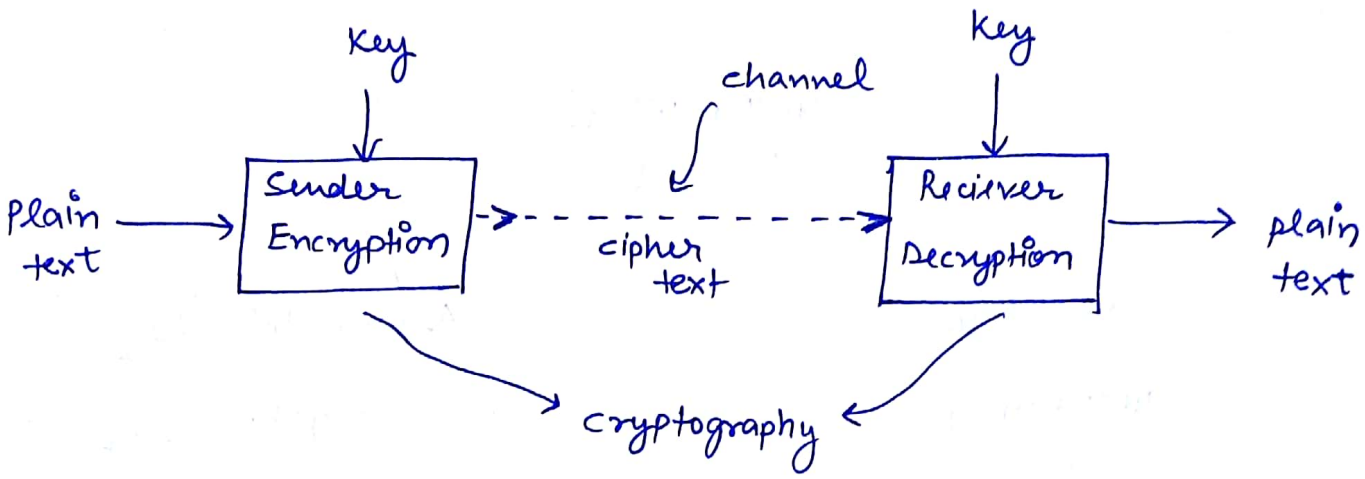


encoded mail = qvi

- Mails can be kept in hierarchy in case of IMAPy whereas all mails are equal or serial in case of POP3.

- Security to the mails like antivirus are provided by IMAPy but not by POP3.

Basics of Network Security :-



- Cryptography is a science of art of converting one form of data into other form to provide security to the data.

- Whenever the key is transmitted on the channel it is known as the public key. When the key is kept as secret it is known as private key.

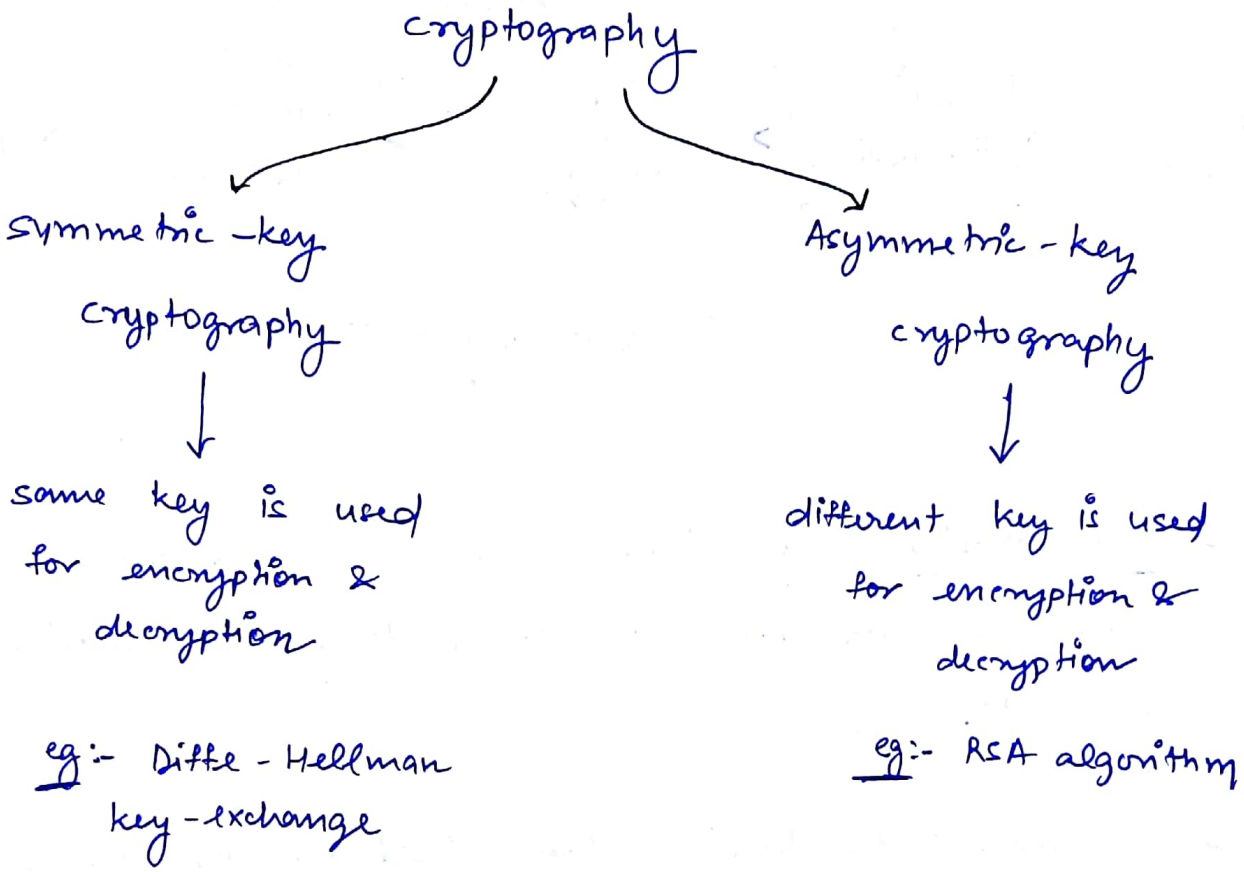
challenges of cryptography -

↳ confidentiality

↳ Authentication

- Providing ~~secracy~~ secracy to the data is called confidentiality.

- Proving user's identity or the integrity of user is known as authentication.



Key-features of cryptography :-

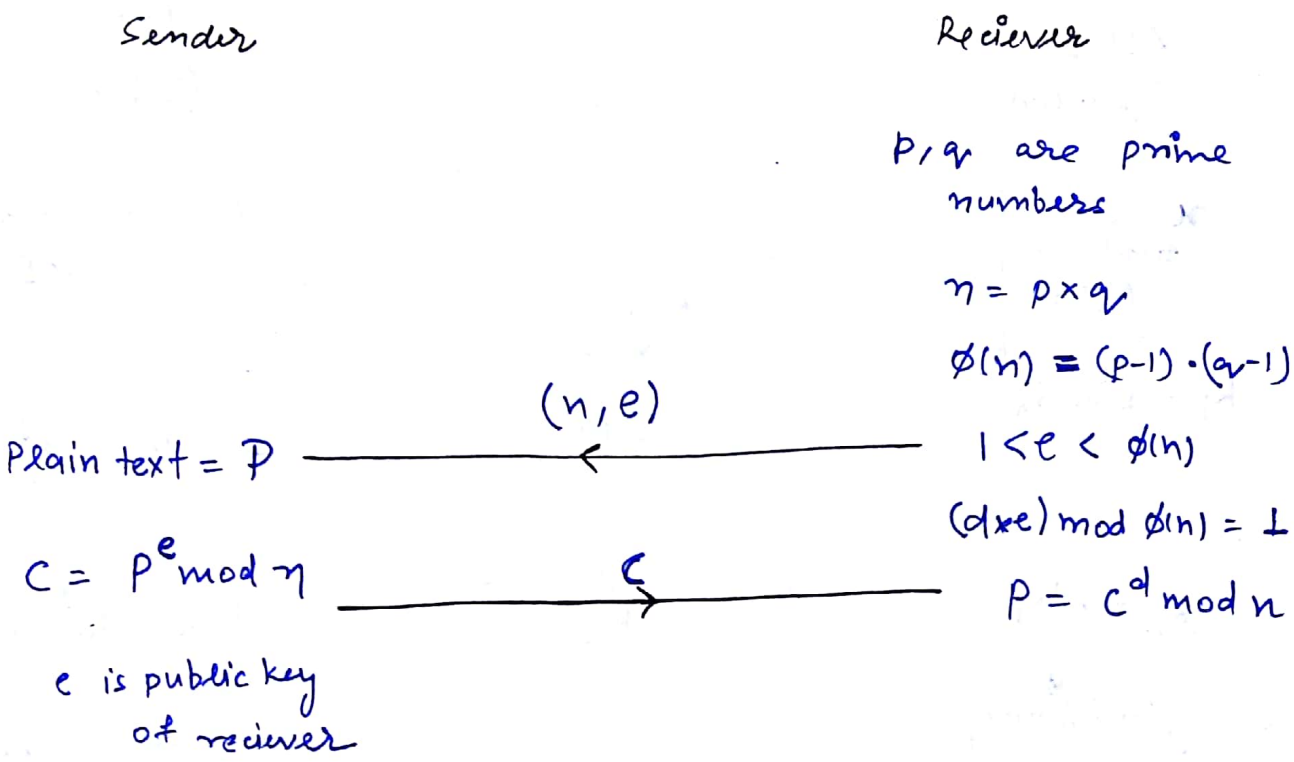
(i) prime numbers

(ii) Random numbers

(iii) Key

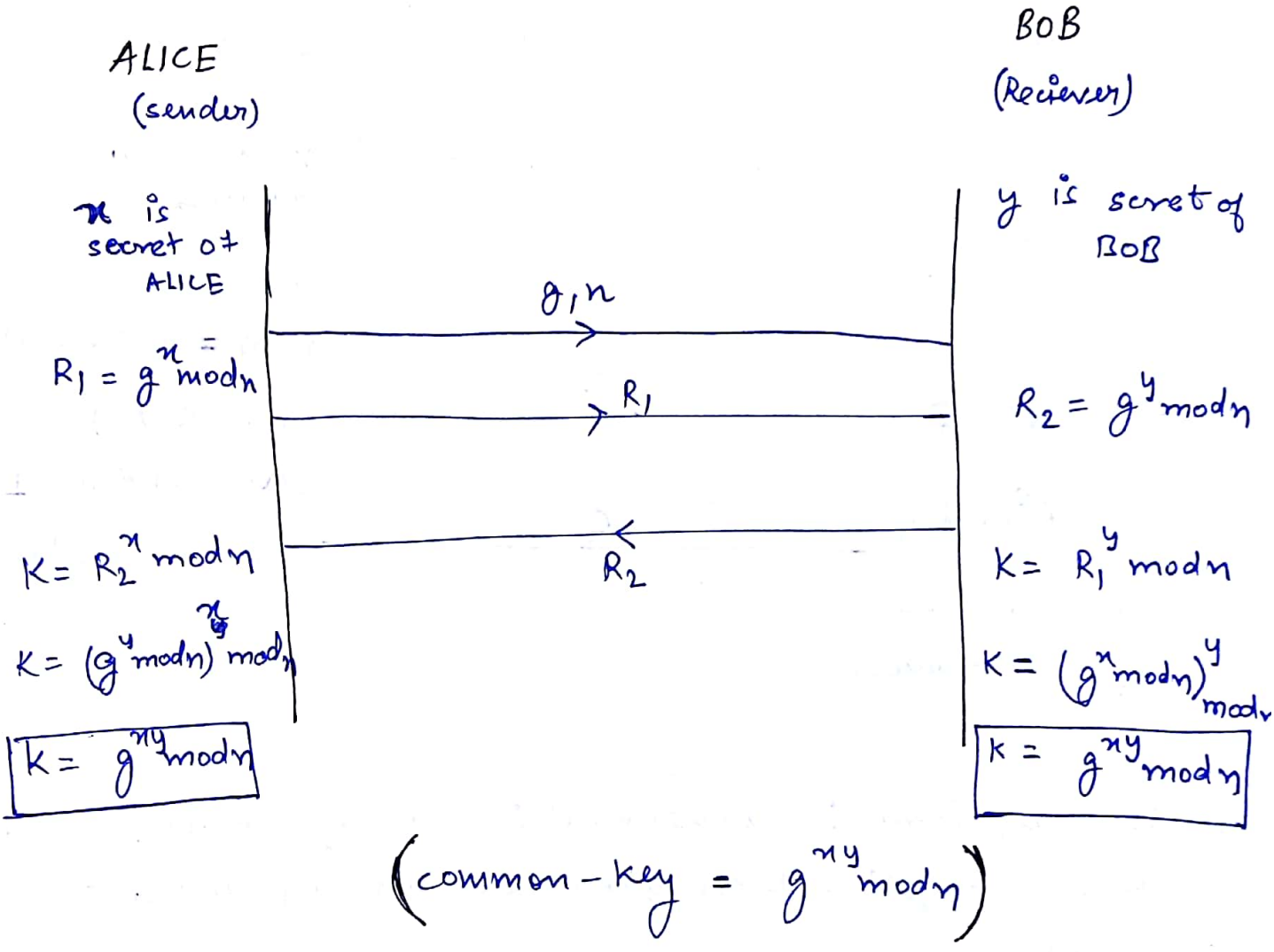
(iv) Timestamp

RSA algorithm :-



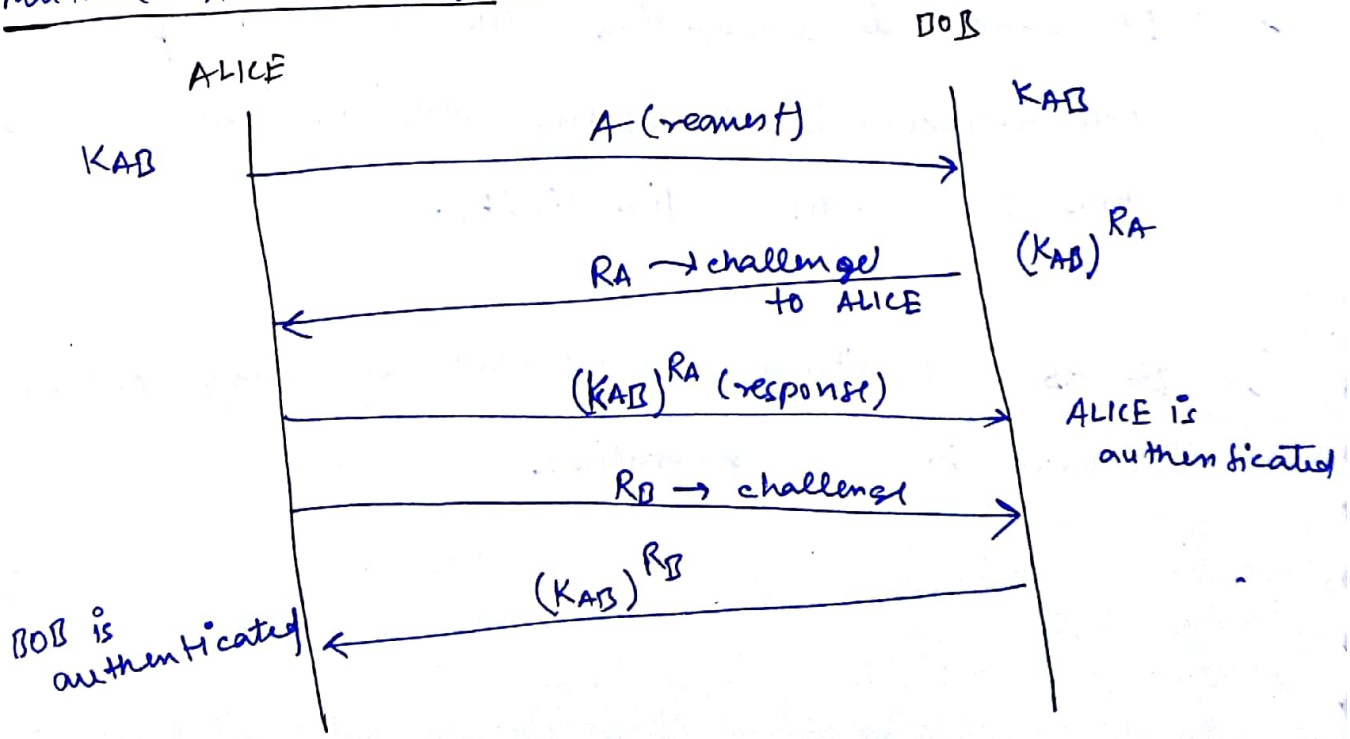
- RSA algorithm is an asymmetric-key cryptography because both encryption & decryption are done by different keys.
- If sender is encrypting with reciever's public key and reciever is decrypting with its own private key, thus it provides confidentiality.
- In RSA algorithm involvement of only one system is there in key generation.

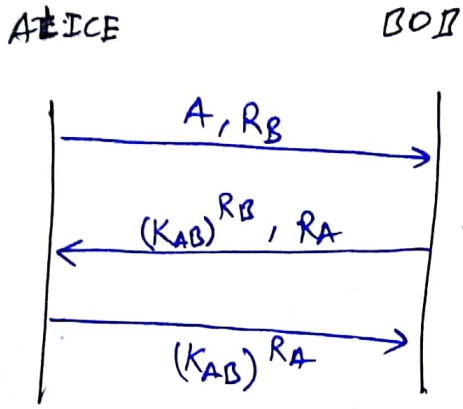
Diffe - Hellman Key exchange :-



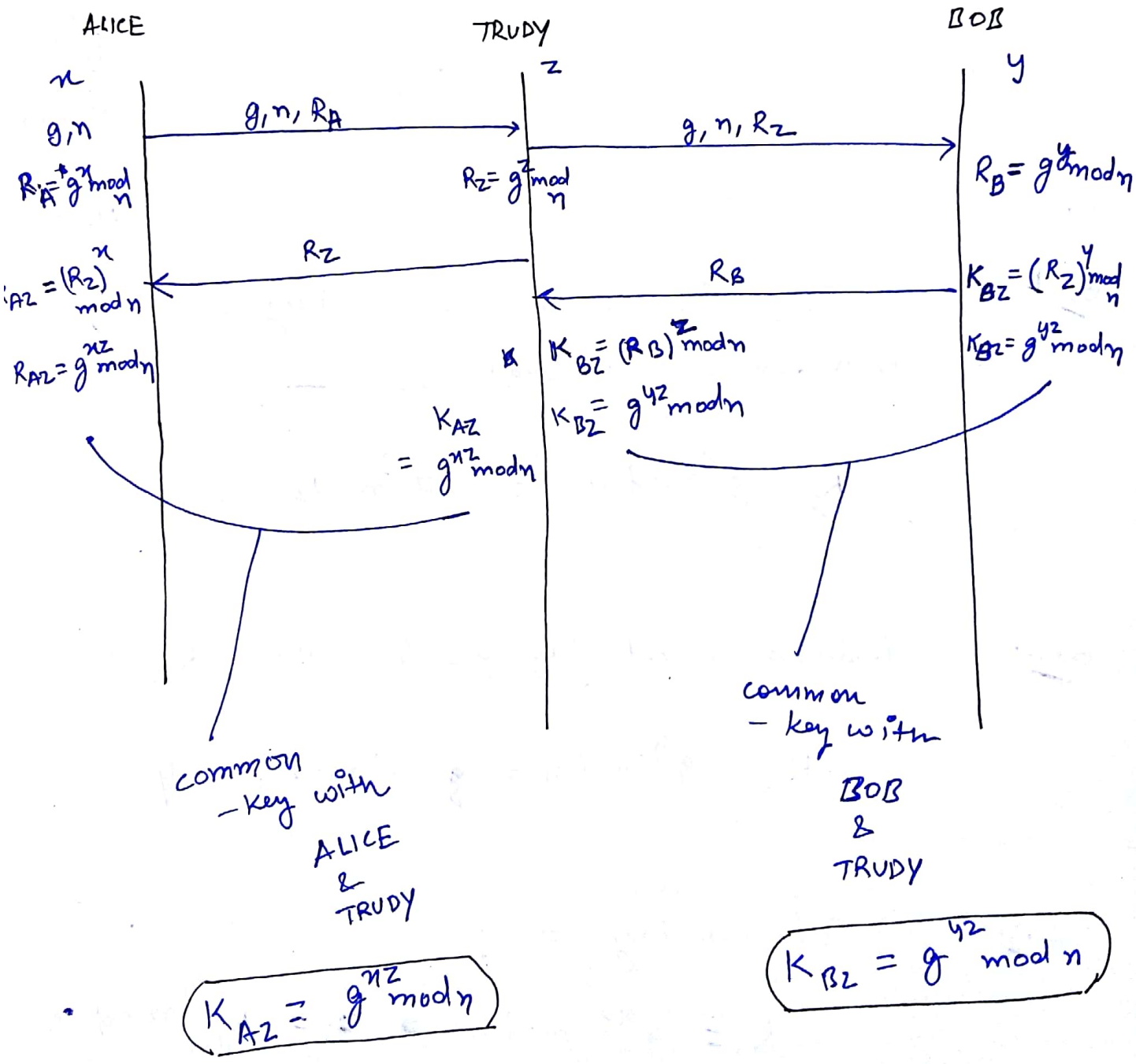
$$\left(\text{common-key} = g^{xy} \bmod n\right)$$

Mutual Authentication :-

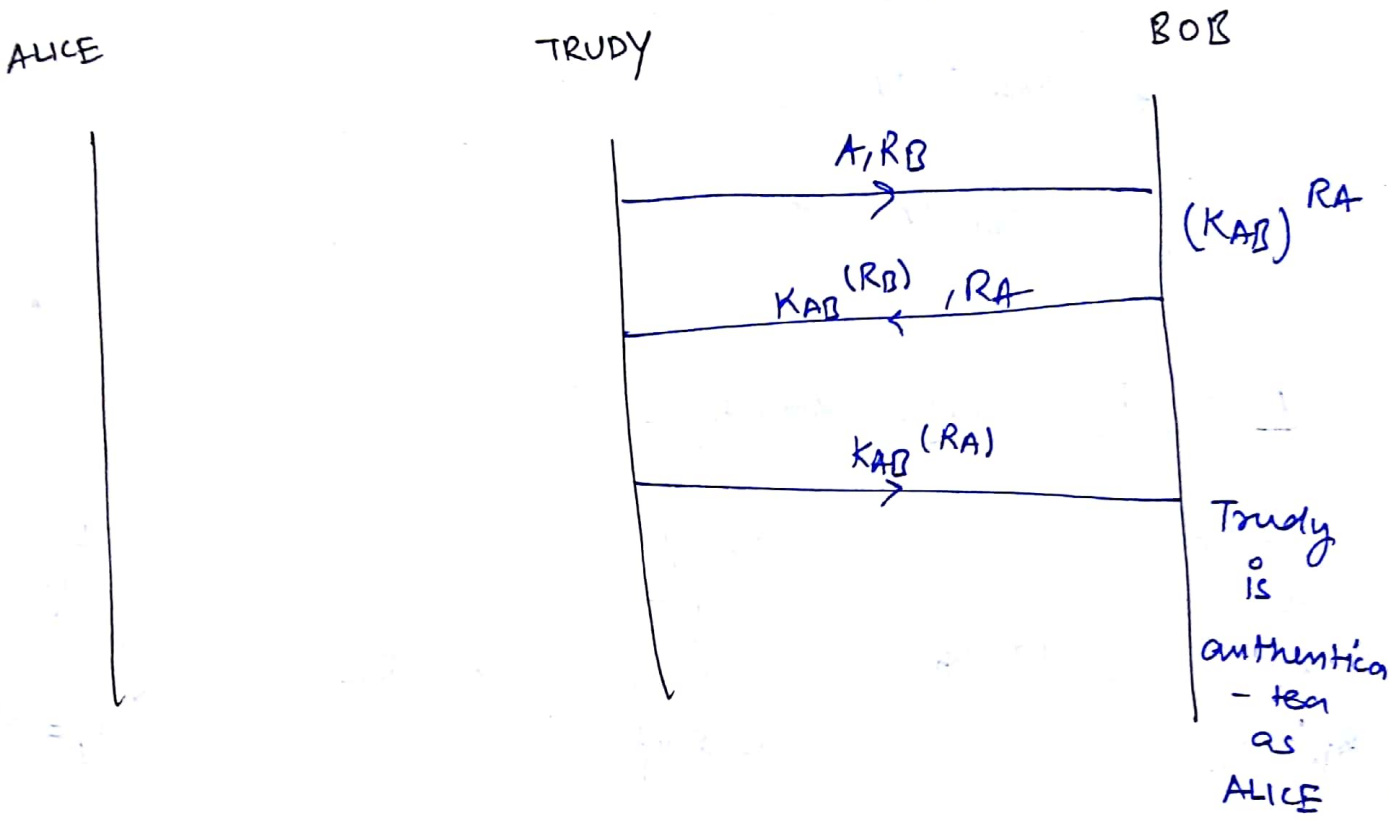




Man-in-Middle Attack :-



Reflection Attack :-



Q.1 $n = 23$, $g = 7$, sender's secret key is $x = 3$, then transmits message (23, 7, ___)

$$R_S = g^x \bmod n = 7^3 \bmod 23 = 21$$

Q.2. Recievers secret key $y = 6$ then R_R ?

$$R_R = g^y \bmod n = 7^6 \bmod 23 = 4$$

Q.3. Common key = ?

$$K = g^{xy} \bmod n = R_R^x \bmod n$$
$$= 4^3 \bmod 23 = 18$$

Q. RSA algorithm :-

$p = 7$, $q = 11$

$n = pq = 77$

$\phi(n) = 6 \times 10 = 60$

$e = 7$

$de \bmod \phi(n) = 1$

Use extended euclidean theorem -

$$ex + \phi(n)\, y = 1$$

$$7x + 60y = 1$$

$60 = 7 \times 8 + 4$ $\quad = \quad 60 - 7 \times 8 = 4$ (i)

$7 = 4 \times 1 + 3$ $\quad = \quad 7 - 4 \times 1 = 3$ (ii)

$4 = 3 \times 1 + 1 \Rightarrow \quad 4 - 3 \times 1 = 1$

$$4 - (7 - 4 \times 1) = 1$$

$$4 - 7 + 4 \times 1 = 1$$

$$4(2) - 7 = 1$$

$4(2) - 7 = 1$

$(60 - 7(8))(2) - 7 = 1$

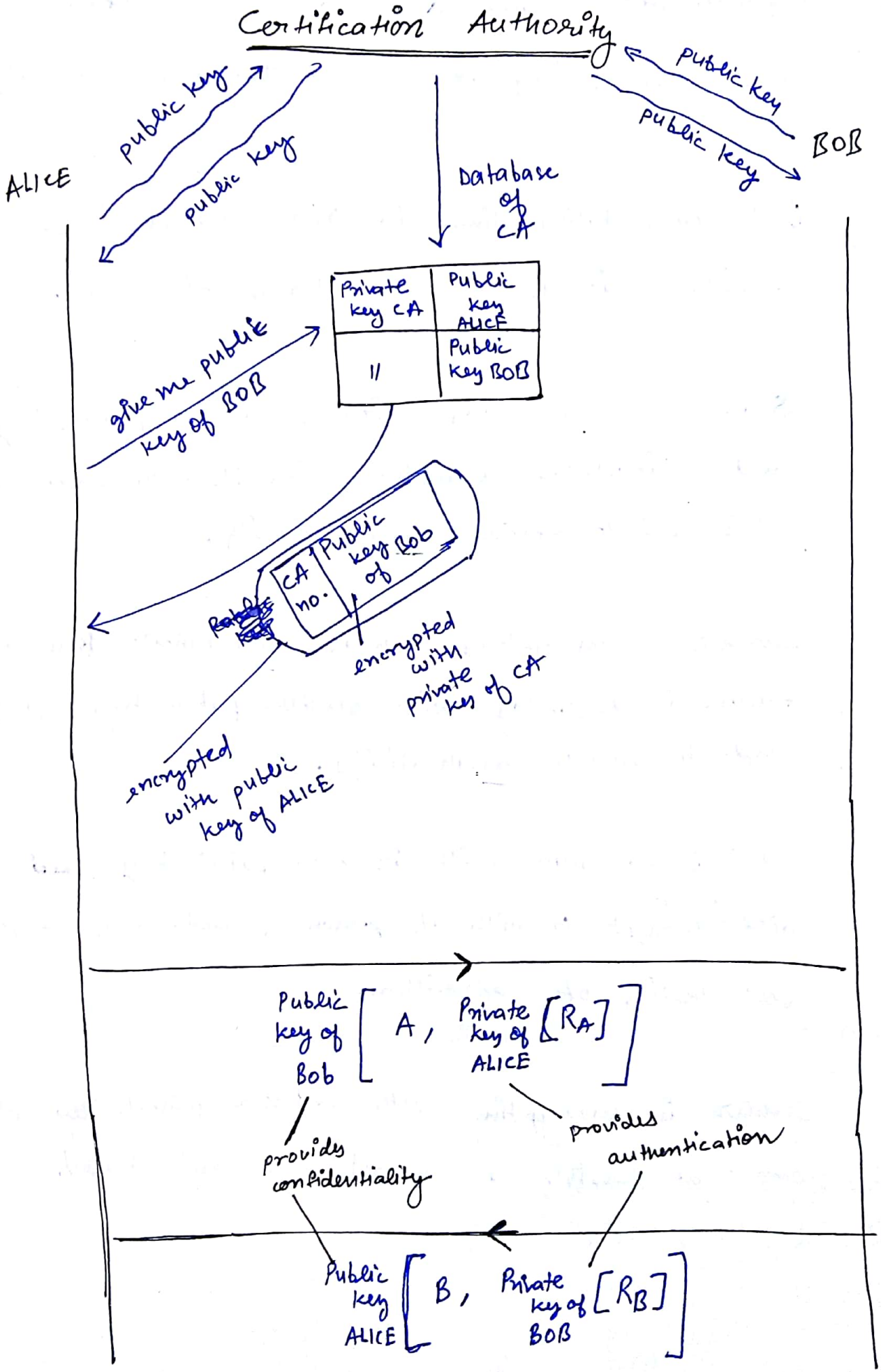
$60(2) - 7(16) - 7 = 1$

$60(2) - 7(17) = 1$

$60(2) + 7(-17) = 1$

60
−17
43

$\boxed{d = 43}$ ✓



- Authentication using RSA algorithm is better than Diffe-Hellman key exchange in terms of security.

- But computation time in Diffe Hellman key is less so it is better in terms of speed.

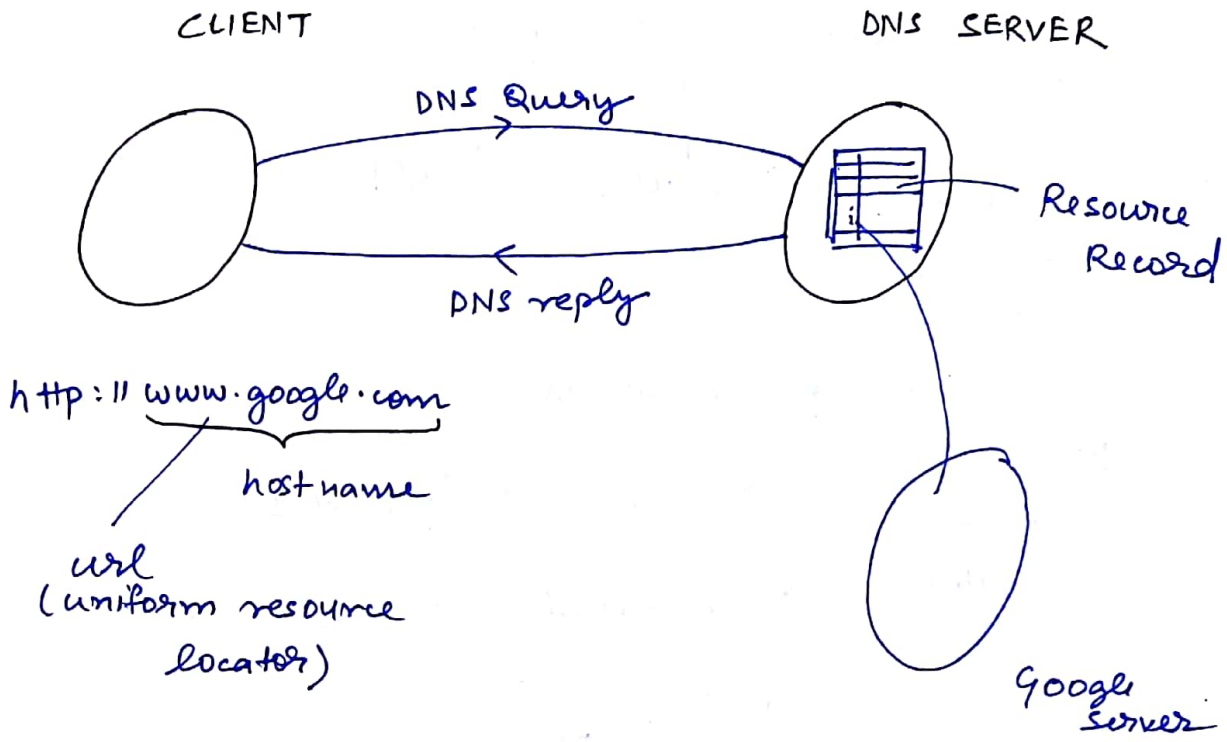
- Sender is encrypting with recivers public key and reciever is decrypting with its own private key. It is used to provide confidentiality.

- Sender is encrypting with its own private key and reciever is decrypting with sender's public key, it is used to provide authenticity.

- Sender is encrypting with its own public key, and will only decrypt it with its own private key for self testing of algorithms.

- Sender is encrypting with reciever private key which can't be possible as private key can't shared.

DNS (Domain Name space) :-



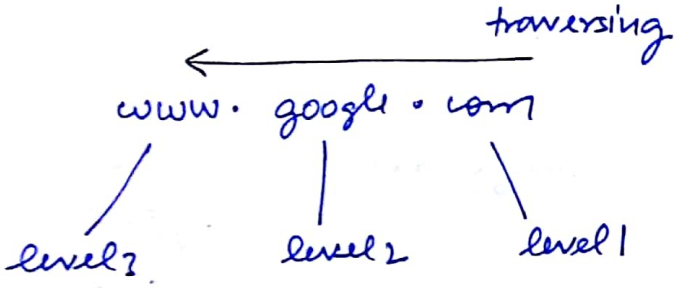
- It is used for converting host name into IP addresses or we can say it is used for mapping hostnames to IP addresses or vice-versa.

Design or Architecture of DNS server :-

(i) DNS servers should be placed in heirarchy so that searching time is less.

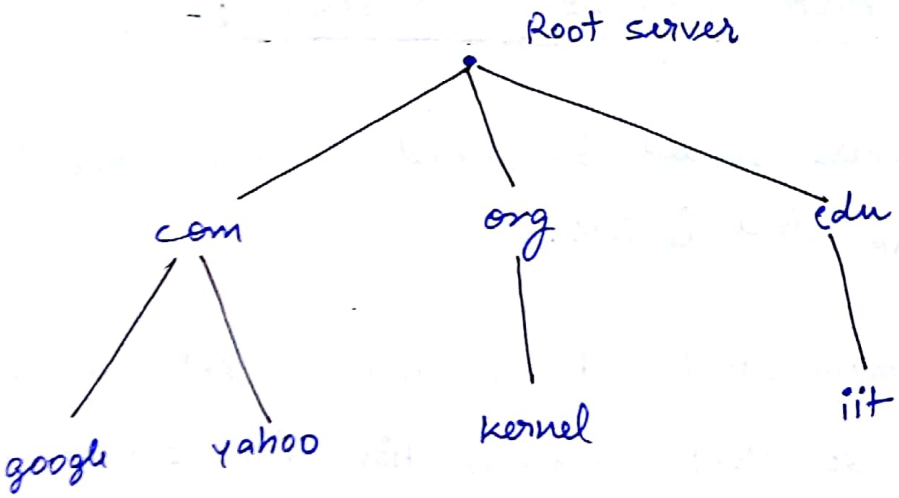
(ii) DNS server should be placed in different part of country so that propagation time should be less.

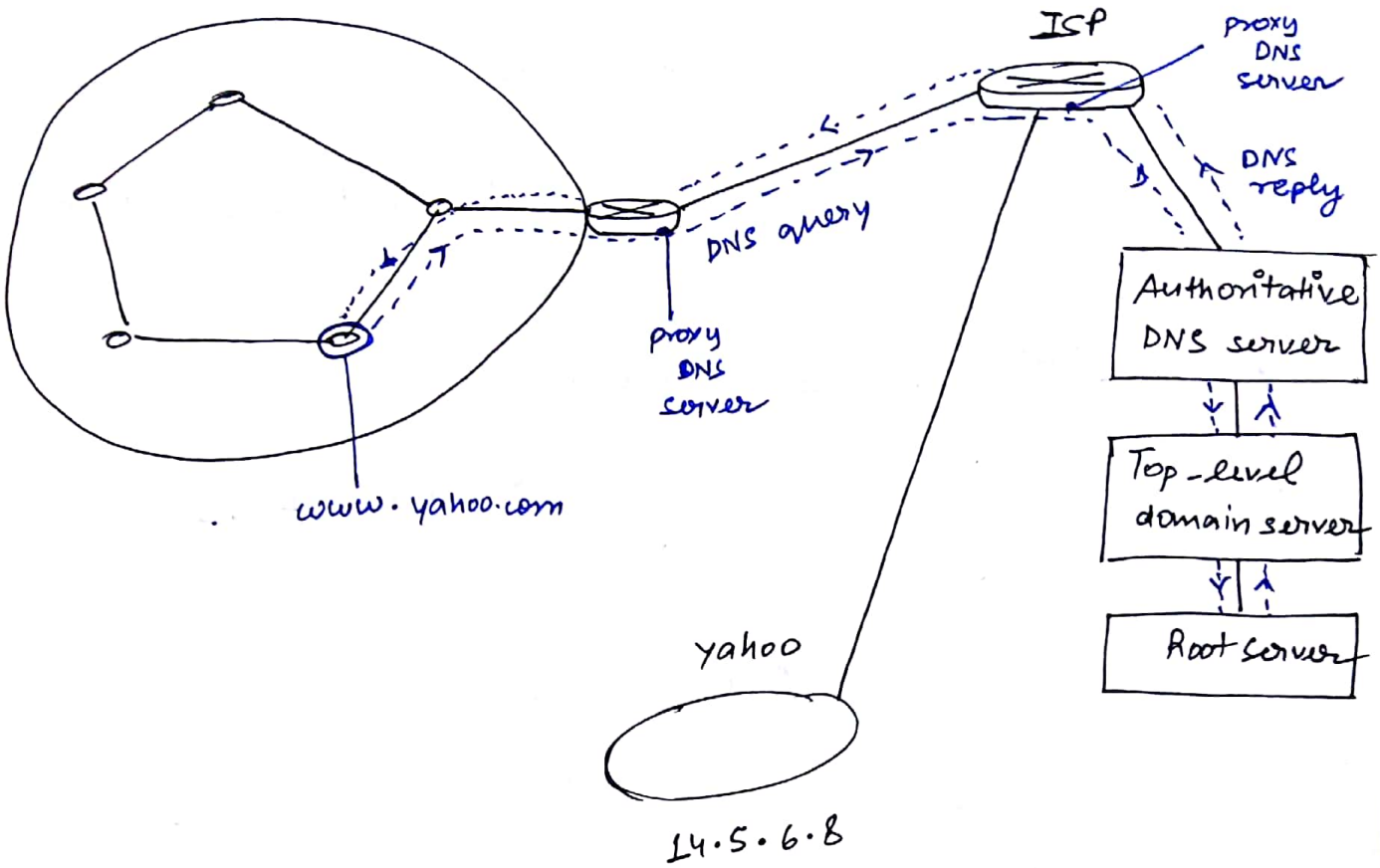
- DNS query size → 127 levels (maximum)



DNS servers hierarchy
- Root servers
- Top-level domain servers
- Authoritative servers
- Local DNS servers or proxy DNS server

eg:-
www.google.com
www.yahoo.com
www.kernel.org
www.iit.edu





- Proxy DNS server (Local routers) will save the DNS reply of some popular website servers url.

  TTL ≥ 24 hrs ; stable record

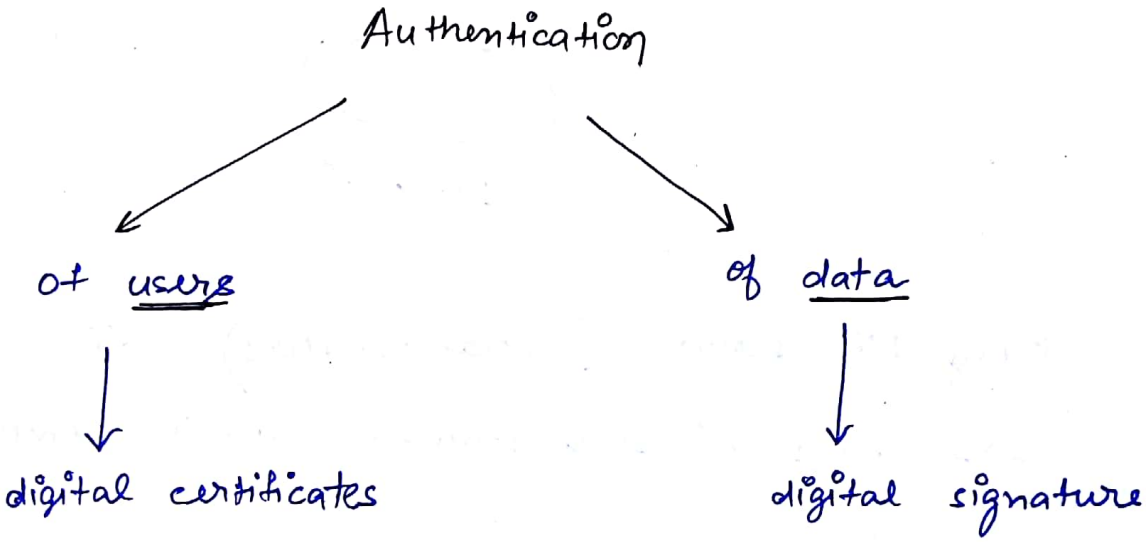
  TTL < 24 hrs ; unstable record

- It is application level protocol.

- It uses UDP at Transport layer as it is fast and it support multicasting, so every node at DNS servers will ~~see~~ send reply and at ISP router or Local DNS server all reply are compared, if they are same than it is forwarded.

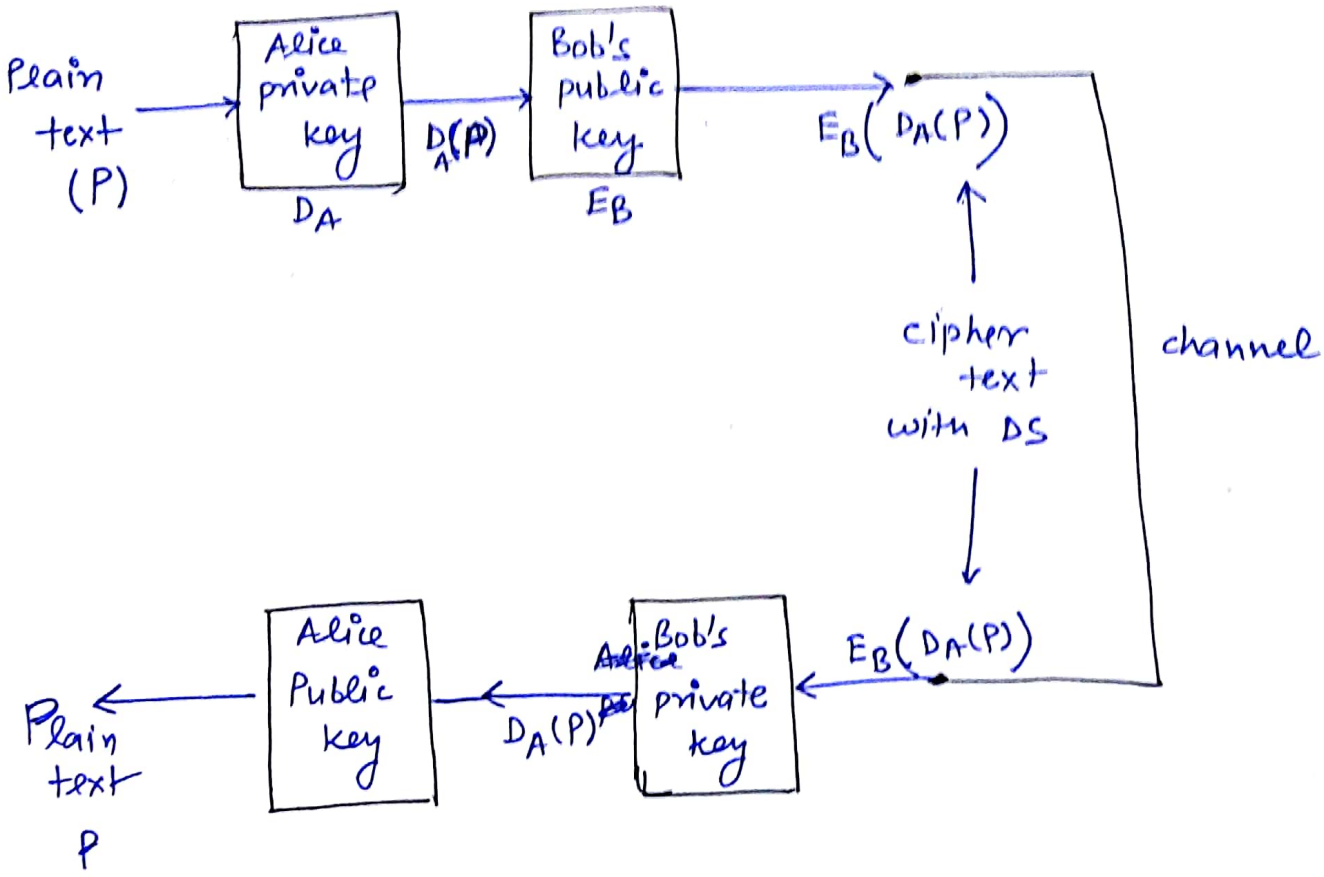
- DNS query ≥ 512 bytes → TCP is used at TL

- DNS query ≤ 512 bytes → UDP at T.L



- In case of hand written signatures for all types of data same signature is used whereas in digital signatures for every individual data a seperate signature is created.

- In case of handwritten signatures both data & signature can't be seperated, whereas in case of digital signatures both data and signature can be seperated.



- Sender will sign the message using its own private key and the verification of the message is done by sender's public key to provide authentication of the data.