Attacks

Active : Make modification
          In data also

Passive : only reads data
          observe communication
          Don't modify
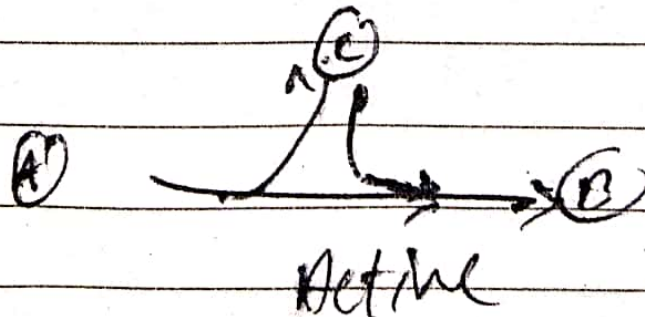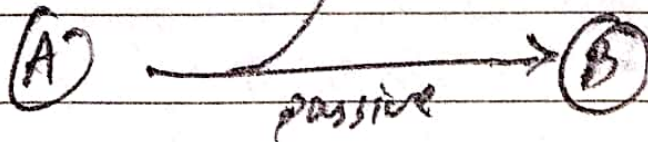
Passive attack:

    ↳ Relase of msg content
       to unauthorized person

   so ↳ no confidentiality

      ↳ Traffic analysis

Active Attacks:

(A) ⟶ ↑©↘ (B)
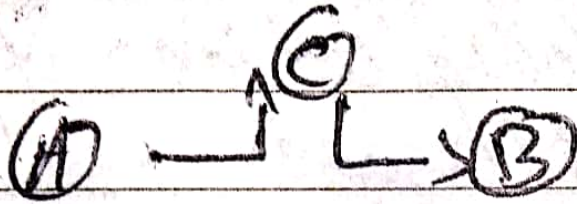
⤷ Masquerade

⟹ gets user name
and password of
sender / confidential
info and sends
messages as (A)

⟹ use services of (A)
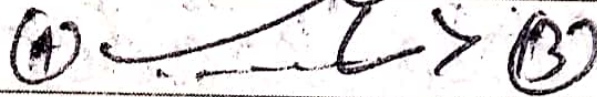
⟹ resources of (A)

⟹ Alter data of (A)

Relay:

⤷ Modification of Message

(A) ⟶ ⟶ (B)

⤷ induce error bits

⤷ sends corrupted data to reciever

⤷ No confidentility

⤷ No integrity

DOS:

→ Deniel of Servics

→ continous request of resources

→ unnecessary packets

→ Causes network to slow down

→ No availasility

Active	Passive
Attacks	Attacks
⇒ modification	no modification
⇒ affects the system	doesn't affect
⇒ Can be detected	Can't be dete
= No/Threat to integrity & availability	⇒ Threat to Confidentiality
⇒ Capture physical control over link and modifies	⇒ Just observe Transmission
⇒ Detection	Prevention

Security Mechemisim

1) Encipherment:

Hiding data using diff Techniques.
Maintain confidentiality

2) Digital Signature:

use for authentication and guarantees integrity using private & public key

(iii) Access Control:

=> limited accessess

=> manage access controls

=> limited permission to access specific data

(iv) Authentical Exchange:

=> assigning authentication to a trusted user

=> by exchanging continous messages

=> and assign as authenticated user

→ Traffic Padding:

⤷ policies and mechm
to avoid traffic analysis
⇒ prevent analyzation
of traffic pattern

Traffic: - - - ☐ - - ☐☐ - - - ☐ - - -
Dumy Packets induced
to prevent traffic
analysis

(vi) Routing Control
⤷ continuously changing
route for traffic so introduce
can't track route.