COL334 Major

Aniruddha Deb

TOTAL POINTS

38.25 / 40

QUESTION 1

1 1.a 3 / 3

✓ + 1 pts Correct packet sequence

1,3,2,5,7,9,4,6,11,8,10,12

or 1,2,3,4,5,7,9,6,8,11,10,12

✓ + 1 pts correct delay calculation

0,2,0,5,0,5,1,4,0,3,0,3 or 1,3,1,6,1,6,2,5,1,4,1,4

or

0,1,1,2,1,5,2,3,1,3,1,3 or 1,2,2,3,2,6,3,4,2,4,2,4

✓ + 1 pts average delay = 23/11 or 34/11 or 23/12 or 35/12

+ 0.5 pts minor mistake in any of the above steps

+ 0 pts Incorrect

QUESTION 2

2 1.b 4 / 4

✓ + 2 pts Correct packet sequence

1,2,4,3,6,8,5,10,12,7,9,11 or 2,4,1,6,3,8,5,10,12,7,9,11

or 2,4,3,6,7,8,9,10,12,11,5,1 or

1,2,4,7,6,8,9,10,12,11,5,3

or 2,1,4,6,3,5,8,7,10,9,12,11 or 1,2,4,3,6,5,8,7,10,12,9,11

✓ + 1 pts correct delay calculation

0,1,2,1,3,2,6,0,5,0,3,0

or

1,2,3,2,4,3,7,1,6,1,4,1

✓ + 1 pts Average delay = 23/11 or 23/12 or 34/11 or 35/12

+ 0.5 pts minor mistake in any of the above step

+ 0 pts incorrect

QUESTION 3

3 1.c 3 / 3

✓ + 1 pts Why NAT in today's world(any one point)

✓ + 1 pts Why NAT temporary solution?(any 1 point)

✓ + 1 pts Will NAT stay? no marks without a valid reason.

+ 0 pts otherwise

QUESTION 4

4 2a 4 / 4

✓ + 4 pts Correct initial and final routing table

- 1 pts calculation and computation step incorrect/incomplete/not shown

+ 0 pts Not attempted/incorrect

QUESTION 5

5 2b 2 / 2

✓ + 2 pts correct answer and explanation

+ 0 pts not attempted/Incorrect answer

+ 1 pts Partially correct answer

QUESTION 6

6 2c 2.25 / 3

✓ + 1 pts How control plane under logical centralized? (SDN concept, remote controller)

✓ + 0.5 pts In such case- Separate devices

✓ + 0.75 pts Any 1 advantage

+ 0.75 pts Any 1 disadvantage

+ 0 pts Incorrect/not attempted

QUESTION 7

7 3a 4 / 5

✓ + 1.5 pts Correctly detecting when the collision happens

Explanation:

we assume both transmit at equal speeds. So, collision happens somewhere in the mid,i.e,

245/2 = 122.50-bit times

✓ + 1.5 pts **Correct usage of the jamming signal.**

Explanation:

Both A and B send and alert each other that a collision has occurred after
245 + 10 = 255-bit times.
next transmission will happen at 255+245 = 500 bit times

+ **2 pts** Reporting the correct packet starting for both A and B.

Explanation:

Since there is only one collision let's assume A takes k=0 and B takes k=1 in the CSMA/CD algorithm.
So, the frame from A starts at 500 bit-time and reaches B at 500+245+300=1045-bit times.
while B will start to send its frame at 1046-bit times.

+ **0 pts** wrong

+ **1 Point adjustment**

wrong start time for B

QUESTION 8

8 3b **3 / 3**

✓ + 3 pts **Correct**

+ **1 pts** Partially Correct/Correct Idea

+ **0 pts** Incorrect/Unattempted

+ **1 pts** Correct Expression but steps not shown/are unclear.

QUESTION 9

9 3c **2 / 2**

✓ + 1 pts **Explained why ARP query is sent in a broadcast frame (the destination MAC address is not known, hence everyone is to be asked)**

✓ + 1 pts **Explained why the response is directed to a specific MAC (the source address is now known from the query, so a broadcast would be wasteful)**

+ **0 pts** Incorrect/Unattempted

QUESTION 10

10 4a **2 / 2**

+ **0 pts** incorrect answer(if answer is yes)

+ **1 pts** Answer is No, but partially correct explanation

✓ + 2 pts **Answer is No, and correct explaination**

QUESTION 11

11 4b **3 / 3**

+ **0 pts** Totally Incorrect answer

+ **1.5 pts** Correct explanation of how message reaches but without explaining the role of HSS,MME or gateway routers in it or incorrect explanation of some part or some missing detail

✓ + 3 pts **All parts included**

- **0.5 pts** for frivolous regrade request

QUESTION 12

12 4c **3 / 3**

✓ + 1 pts **Fully correct for confidentiality**

+ **0.5 pts** Partially correct for confidentiality

✓ + 1 pts **Fully correct for authentication**

+ **0.5 pts** Partially correct for authentication

✓ + 1 pts **Correct example Provided(for both confidentiality and authentication)**

+ **0.5 pts** Partially correct example or lacks explanation

+ **0 pts** Wrong answer

QUESTION 13

13 4d **3 / 3**

✓ + 1 pts **Correct definition of attack**

✓ + 0.5 pts **Correct example explaining working of attack**

✓ + 1.5 pts **Correct Prevention technique with role of CA**

+ **0.5 pts** Only prevention (CA role not mentioned)

+ **0 pts** No attempt

Indian Institute of Technology Delhi
Department of Computer Science and Engineering
COL334/672: Computer Networks
Major Examination, Diwali 2022

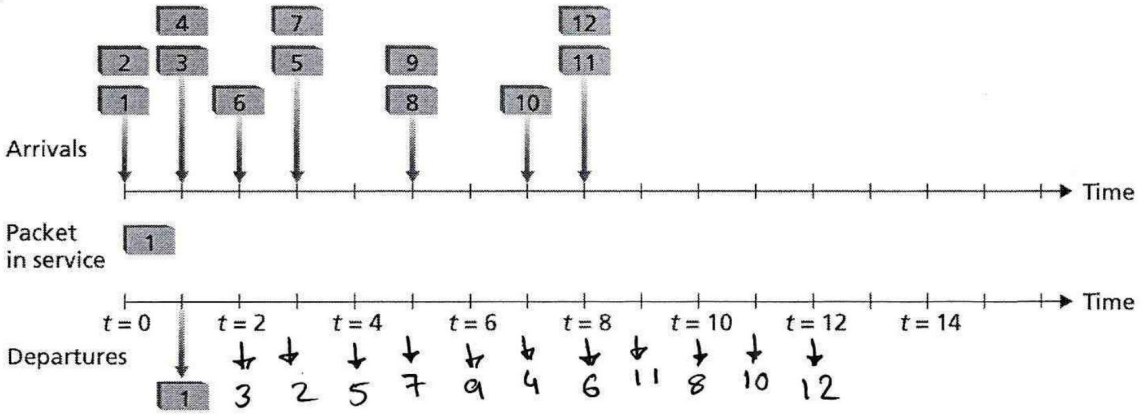
Full Marks: 40 **Time: 2 hours**

Name ANIRUDDHA DEB **Entry Number** 2020CS10869

Answer the questions on the space provided
Be precise in your answers, and state any assumptions made

Question 1 [3+4+3 = 10 marks]

(a) Consider the following packet arrival pattern in a router. Assume that the router follows a priority-based scheduling policy where odd-numbered packets are high priority, and even-numbered packets are low priority. If only one packet can be transmitted during one timeslot, indicate the time at which packets 2 through 12 each leave the queue. What is the average delay between a packet's arrival and the beginning of the slot in which it is transmitted? Show the computation steps.



H.P

t=1 : 1 → 1

2

L.P

t=2 : 3 → 3

4 2

t=3 : → 2

6 4 2

t=4 : 7 5 → 5

6 4

t= 5 : 7 → 7

6 4

t=6 : 9 → 9

8 6 4

t= 7 : 8 6 4 → 4

t= 8 : 10 8 6 → 6

t=9 : 11 → 11

12 10 8

t= 10 : 12 10 8 → 8

t=11 : 10

t=12 : 12

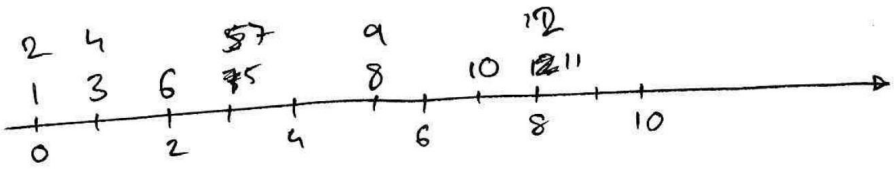
∴ time spent in router :

2 - 3 s
3 - 1 s
4 - 6 s
5 - 1 s
6 - 6 s
7 - 2 s
8 - 5 s
9 - 1 s
10 - 4 s
11 - 1 s
12 - 4 s

$$\therefore \text{avg. delay} = \frac{3+1+6+1+6+2+5+1+4+1+4}{11}$$

$$= \frac{34}{11}$$

$$= \boxed{3.09 \text{ s}}$$



(b) Consider the same packet arrival pattern as shown in the previous figure. However, instead of priority-based, now assume that the router is following a weighted fair queueing (WFQ) scheduling policy. Further assume that odd-numbered packets are from Class 1 having WFQ weight of 1, and even-numbered packets are from Class 2 having WFQ weight of 2. Indicate which packet will go into service at each time slot. What is the average delay between a packet's arrival and its departure in this scheme? Show the steps clearly.

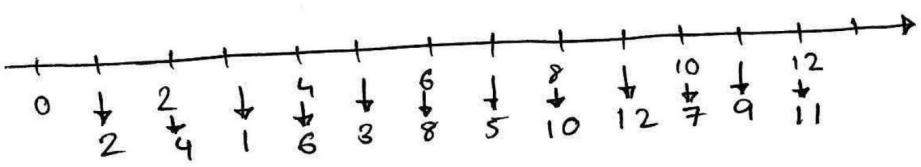
odd, $w=1$; even, $w=2$

$t=1$: 1, 2 → 2 $\quad$ $t=2$: 3, 1, 4 → 4 $\quad$ $t=3$: 3, 1, 6 → 1

$t=4$: 7, 5, 3, 6 → 6 $\quad$ $t=5$: 7, 5, 3 → 3 $\quad$ $t=6$: 9, 7, 5, 8, 8 → 8

$t=7$: 9, 7, 5 → 5 $\quad$ $t=8$: 9, 7, 10 → 10 $\quad$ $t=9$: 11, 9, 7, 12 → 12

$t=10$: 11, 9, 7 → 7 $\quad$ $t=11$: 11, 9 → 9 $\quad$ $t=12$: 11 → 11



$t_2 = 1$ $\quad$ $t_5 = 4$

$t_4 = 1$ $\quad$ $t_{10} = 1$

$t_1 = 3$ $\quad$ $t_{12} = 1$

$t_6 = 2$ $\quad$ $t_7 = 7$

$t_3 = 4$ $\quad$ $t_9 = 6$

$t_8 = 1$ $\quad$ $t_{11} = 4$

$$\text{avg} = \frac{35}{12} = \boxed{2.92 \text{ s}}$$

(c) What is the need for Network Address Translation (NAT) in today's internet? Why was NAT considered to be a temporary solution? Do you think NAT will stay in operation in foreseeable future? Why?

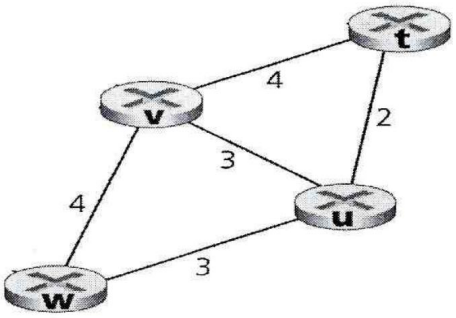
i) NAT is needed as the 32-bit IP address space is too small to accomodate all the hosts that may connect to the internet today and assign each a unique IP.

ii) NAT was considered temporary as the router has to intercede the packets being sent and change the ~~IP~~ destination IP and port for each packet; this is infeasible & slow for a large no. of packets, and also as nodes scale. ~~NAT also requires +~~

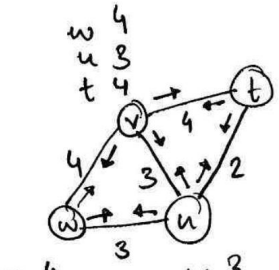
iii) NAT will stay in operation till the ~~network~~ internet transitions over completely to IPv6, as IPv6 has ~~enough~~ a large enough address space to give each device a unique IP address.
(128 bits long)

Question 2 [4+2+3 =9 marks]

(a) Consider the network shown in the figure below and assume that each node initially knows the costs to each of its neighbors. Consider the distance-vector algorithm and compute the distance table entries at each node. Show the computation steps.

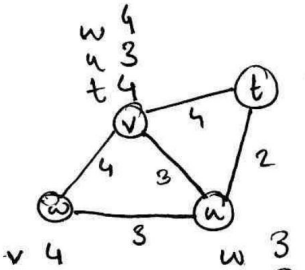


t=0:



u 2
v 4
w ∞

t = 1 :



u 2
v 4
w 5

after t = 1, the router tables converge and no updates happen.

∴ The final routing tables are:

w: v - 4, u - 3, t - 5

u: w - 3, v - 3, t - 2

v: w - 4, u - 3, t - 4

t: u - 2, v - 4, w - 5

Computation steps for t = 1:

w: $d(v) = \min(d(v), c(u,w) + d(u,v)) = \min(4, 6) = 4$

$d(u) = \min(d(u), c(v,w) + d(u,v)) = \min(3, 7) = 3$

$d(t) = \min(d(t), c(w,v) + d(v,t), c(w,u) + d(u,t)) = \min(\infty, 8, 5) = 5$

v: $d(w) = \min(d(w), c(v,t) + d(t,w), c(u,v) + d(u,w)) = \min(4, 6, 6) = 4$

$d(u) = \min(d(u), c(w,v) + d(w,u), c(v,t) + d(t,u)) = \min(3, 7, 6) = 3$

$d(t) = \min(d(t), c(v,w) + d(w,t), c(w,v) + d(w,t)) = \min(2, 7, 7) = 2$

u: $d(w) = \min(3, 3+4, \infty) = 3$

$d(v) = \min(3, 3+4, 2+4) = 3$

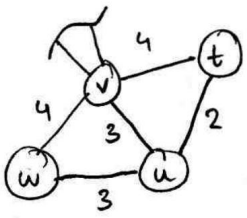
$d(t) = \min(2, 3+4, 3+\infty) = 2$

t: $d(u) = \min(2, 4+3, \infty) = 2$

$d(v) = \min(4, 3+2, \infty) = 4$

$d(w) = \min(\infty, 2+3, 4+4) = 5$

(b) Assume that the nodes in the figure are connected to other nodes in the network (not explicitly shown). Give link-cost change for the links (u,t) and (u,w) such that node v will inform its neighbors of new paths as a result of executing the distance-vector algorithm.



v: w - 4

u - 3

t - 4

i) for new paths to t via (u,t), we need

$c(v,u) + D(u,t) < 4 \Rightarrow D(u,t) < 1$

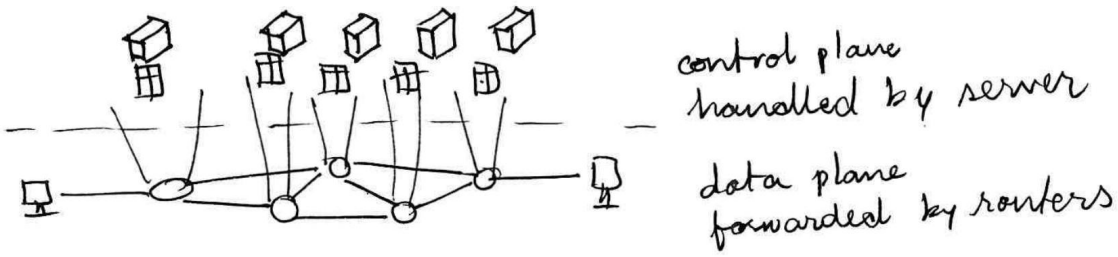
setting (u,t) to $\boxed{0.5}$ will cause v to update it's neighbours. Any value between 0 & 1 is acceptable

ii) Similarity, for new path to w via (u,w), we need $c(v,u) + D(u,w) < 4 \Rightarrow D(u,w) < 1$.

Setting (u,w) to $\boxed{0.5}$ will cause v to update it's neighbours. Any value between 0 & 1 is acceptable. (Link-cost has to be > 0)

(c) How can a control plane be under logically centralized control? In such cases, are the data and control planes implemented within the same device or in separate devices? What are the advantages and disadvantages in such approach? Precisely explain your answer.

i) In Software Defined Networking (SDN), we can have the control planes of all the routers in a network processed/updated in a centralised server, which updates the routers' routing tables via a ~~network~~ connection.



ii) The data plane is implemented in the router: the router has forwarding tables enabling it to forward incoming data to the final destination.

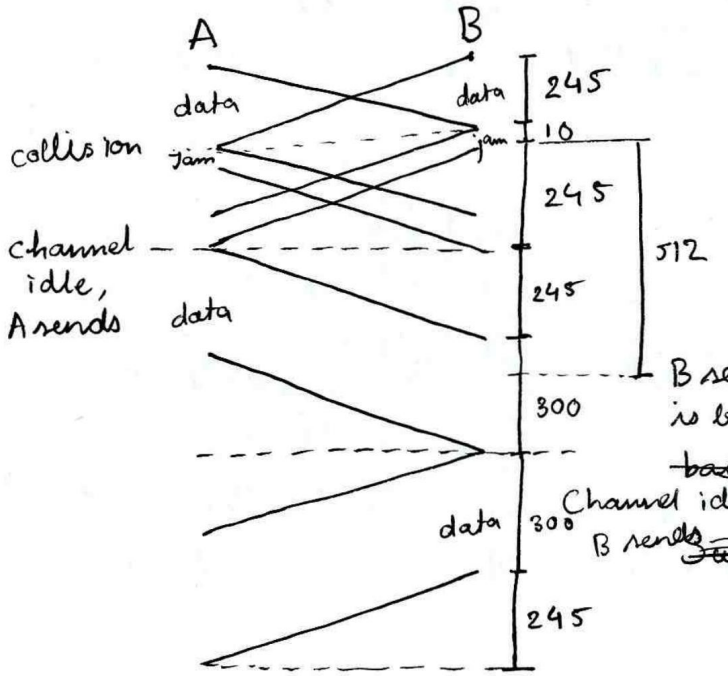
The control plane is implemented in ~~servers and into software~~ Software running on centralized servers: the servers compute optimal routing policies and install the forwarding tables on routers via a connection to them.

∴ These planes are implemented in separate devices

iii) SDN allows for more optimal network traffic flow, as the server knows the traffic and flow statistics at each node and can load balance optimally and update the tables of routers in real time.

Question 3 [5+3+2 = 10 marks]

(a) Two nodes A and B are on a 10 Mbps broadcast channel, and the propagation delay between them is 245 bit times. Suppose A and B start sending Ethernet frames at the same time, the frames collide, and then A and B choose different values of K in the CSMA/CD *backoff* algorithm. Assuming no other nodes to be active, when can A and B retransmit the frames? Suppose the frame size is 300 bits and the jam signal is 10 bits. Show all computation steps. [Hint: *In CSMA/CD, a node waits K·512 bit times before sensing the channel again*]



Suppose A chooses 0, B chooses 1.

~~backoff again with n=2 (K ∈ {0, 1, 2, 3}).~~

~~Suppose B chooses~~

∴ A can retransmit after $245 + 10 + 245 = 500$ bit times

$= \frac{500}{10 \times 10^6} = \frac{1}{2} \times 10^{-4}$

$= \boxed{50\ \mu s}$ (after t=0)

B can retransmit after $500 + 245 + 300 = 1045$ bit times

$= \boxed{104.5\ \mu s}$ (after t=0).

(b) Consider a broadcast channel with N nodes and a transmission rate of R bps which uses polling for medium access. Suppose the amount of time from when a node completes transmission until the subsequent node is permitted to transmit (the polling delay) is d. Further assume that within a polling round, a given node is allowed to transmit at most M bits. What would be the maximum throughput of this broadcast channel?

Max throughput is when all nodes transmit M bits the extra overhead bits (for polling) are RdN (polling N nodes for d duration on a link R bps).

$\therefore$ Throughput = $\frac{\text{bits}}{\text{time}}$

$$= \frac{NM}{\frac{NM}{R} + \frac{RdN}{R}} = \frac{NM}{\frac{NM}{R} + dN} = \frac{M}{\frac{M}{R} + d}$$

$$= \boxed{\frac{MR}{M + dR} \text{ Bits/sec}}$$

(c) Why is an ARP query sent within a broadcast frame? Why is an ARP response sent within a frame with a specific destination MAC address?

i) An ARP query, the sender doesn't know the MAC address of the recipient, so they broadcast the query to all nodes on the subnet so that the recipient replies. This is analogous to calling out a person's name in a crowded room, so that they may respond and you are able to locate them.

ii) The ARP response is meant for a specific reciver: the host which sent the ARP query (and set the 'sender' field in the query appropriately). Other nodes are not concerned with the MAC address of the recipient, and to prevent extra traffic on the network, the response has a specific destination MAC address.

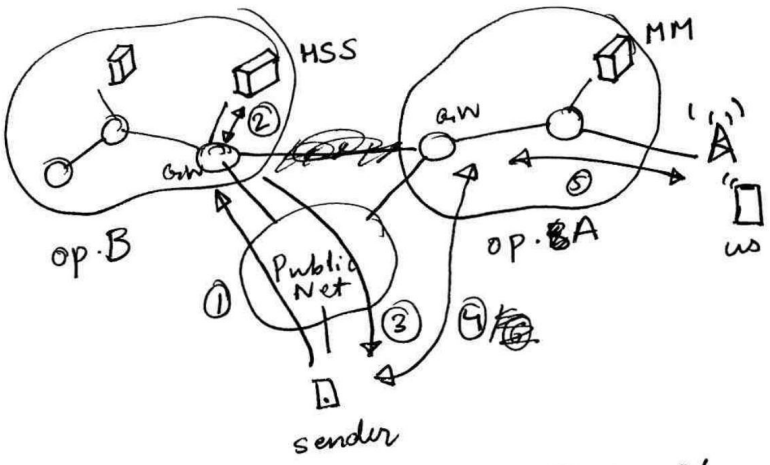
Question 4 [2+3+3+3 = 11 marks]

(a) Suppose the IEEE 802.11 RTS and CTS frames were as long as the standard DATA and ACK frames. Would there be any advantage to using the CTS and RTS frames? Why or why not?

There would not be any advantage to using these frames, as the RTS frames sent by multiple senders would collide with each other and never reach the router. Similarly, if even an RTS manages to reach, the CTS sent by the router may collide with the RTS of a sender because of it's long duration.

Hence, RTS/CTS frames need to be short to avoid colliding with each other.

(b) You travel to an area with coverage from a cellular operator A, but your sim is registered with operator B. If one of your contacts sends you a sms while you are traveling, how would the message be delivered to your phone? Assume Direct Routing is used.



① Sender sends the SMS to operator B's gateway router

② operator B's router requests the HSS for our location: HSS says we're on operator A's network

③ Op. B's router returns to us the address of Op. A's gateway router

④ the SMS is then sent to Op. A's gateway router

⑤ Op. A's router forwards the SMS to us, as we are located on the same network as the router.

(c) How is Public Key Cryptography used for both confidentiality and authentication? Explain using an example.

i) Confidentiality: if Alice has a message m to send to Bob, Alice will encrypt ~~the~~ ~~mess~~ m with Bob's public ~~key~~ ~~private~~ key, K_B^+.
Alice will then send Bob the ciphertext $c = K_B^+(m)$.
Bob will decrypt the ciphertext using his private key K_B^- and obtain the plaintext message $m = K_B^-(c) = K_B^-(K_B^+(m))$.
No other entity will be able to decrypt c, as the private key K_B^- ~~and~~ ~~private~~ is unique to the public key K_B^+, and they don't have K_B^-. Also, it is hard to reverse-engineer and obtain K_B^- from K_B^+ (factoring product of 2 prime numbers as in RSA is hard).
↑ large

~~i) Authentication: Certificate Authorities are used for Authentication: to verify if Alice is indeed the sender, She will encrypt~~

ii) Authentication: To ensure that alice is the sender, Alice will first encrypt the ciphertext with her private key and then with Bob's public key, giving the ciphertext $c = K_B^+(K_A^-(m))$.

Then, Bob will decrypt the ciphertext using his private key and Alice's public key, giving him the message

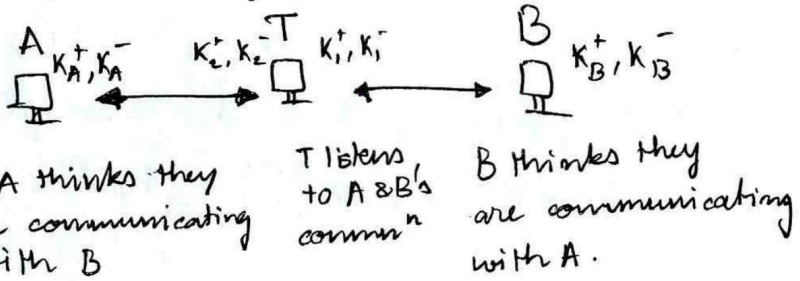
$$m = K_A^+(K_B^-(c)) = K_A^+(K_B^-(K_B^+(K_A^-(m)))) = K_A^+(K_A^-(m)) = m$$

Nobody else can decrypt the message, as they do not have the keys required (Confidentiality) and Only Alice could have sent the message, as the decryption only worked with Alice's public key. (Authentication)

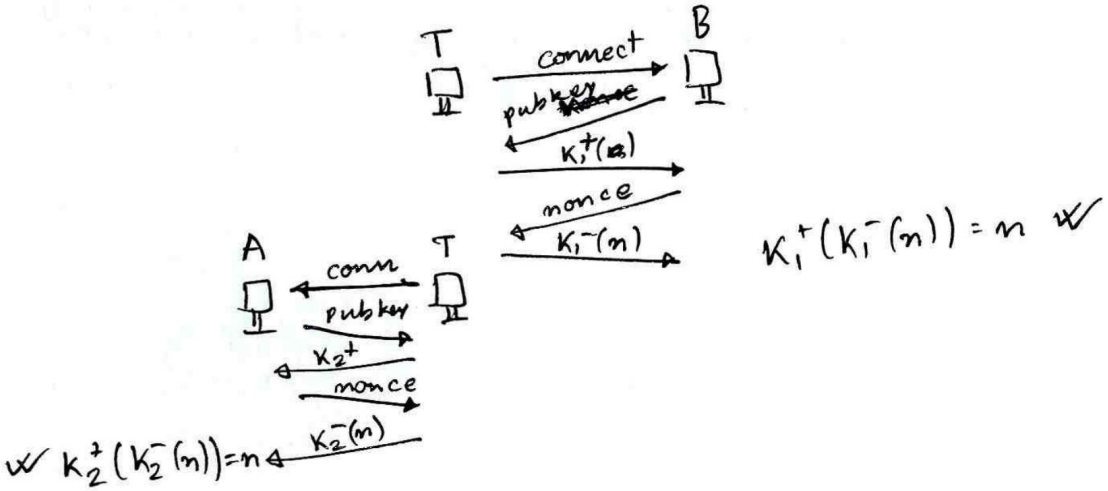
NOTE: This is about authentication in general & not authentication protocols: to ensure an authentication protocol is secure, Certificate authorities are used.

(d) What is man-in-the-middle attack? How can one prevent it? Explain your answer with an example.

A man in the middle (MITM) attack occurs when an intruder T impersonates themselves as B to A and as A to B, and forwards the messages they send while listening to them.



An MITM attack occurs when, in the handshake phase, T handshakes first with B under the guise of being A and vice versa with A.



This can be prevented by using a Certificate Authority (CA): a CA signs the publickey (of a person) with their private key, creating a certificate. This certificate verifies that the sender of this message is the intended sender, and hence T cannot arbitrarily use K_1 & K_2 to impersonate themselves as A and B.