University of Asia Pacific

Department of CSE

Semester Final Examination, Spring 2020

Name: Rashik Rahman

Reg ID: 17201012

Year: 3rd

Semester: 2nd

Course Code: CSE 319

Course Title: Computer Networks

Date: 4.11.2020

"During Examination and upload time I will not take any help from anyone. I will give my exam all by myself."

University of Asia Pacific

Admit Card

Final-Term Examination of Spring, 2020

Financial Clearance	PAID

Registration No : 17201012
Student Name : Rashik Rahman
Program : Bachelor of Science in Computer Science and Engineering

Sl.NO.	COURSE CODE	COURSE TITLE	CR.HR.	EXAM. SCHEDULE
1	CSE 313	Numerical Methods	3.00	
2	CSE 314	Numerical Methods Lab	0.75	
3	CSE 315	Peripheral & Interfacing	3.00	
4	CSE 316	Peripheral & Interfacing Lab	1.50	
5	CSE 317	Computer Architecture	3.00	
6	CSE 319	Computer Networks	3.00	
7	CSE 320	Computer Networks Lab	1.50	
8	CSE 321	Software Engineering	3.00	
9	CSE 322	Software Engineering Lab	0.75	

Total Credit: 19.50

1. Examinees are not allowed to enter the examination hall after 30 minutes of commencement of examination for mid semester examinations and 60 minutes for semester final examinations.

2. No examinees shall be allowed to submit their answer scripts before 50% of the allocated time of examination has elapsed.

3. No examinees would be allowed to go to washroom within the first 60 minutes of final examinations.

4. No student will be allowed to carry any books, bags, extra paper or cellular phone or objectionable items/incriminating paper in the examination hall.
Violators will be subjects to disciplinary action.

This is a system generated Admit Card. No signature is required.

Admit Card Generation Time: 27-Oct-2020 08:43 PM

17201012

Answer to the Q. No. 1(a)

TCP is reliable transport service between sender & receiver. It provides secure connection. On the otherhand UDP is unreliable data transfer protocol between sender and receiver.

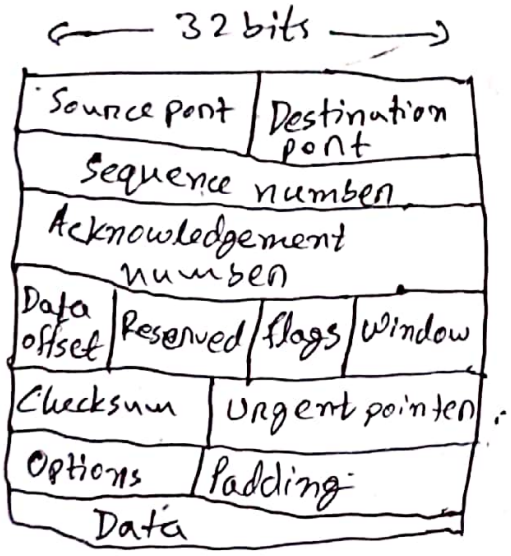


fig: TCP packet

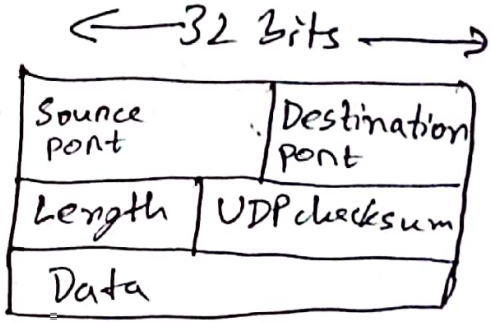


fig: UDP Packet

TCP adds much overhead than UDP thus it makes TCP slower and UDP has less overhead so UDP is fasten. For just making communication to a web server where the only criteria is as fast as possible so I'll definetly choose UDP. If the condition was for secure connection than I would have choose TCP but as it is only as fast as possible so I'll choose UDP.

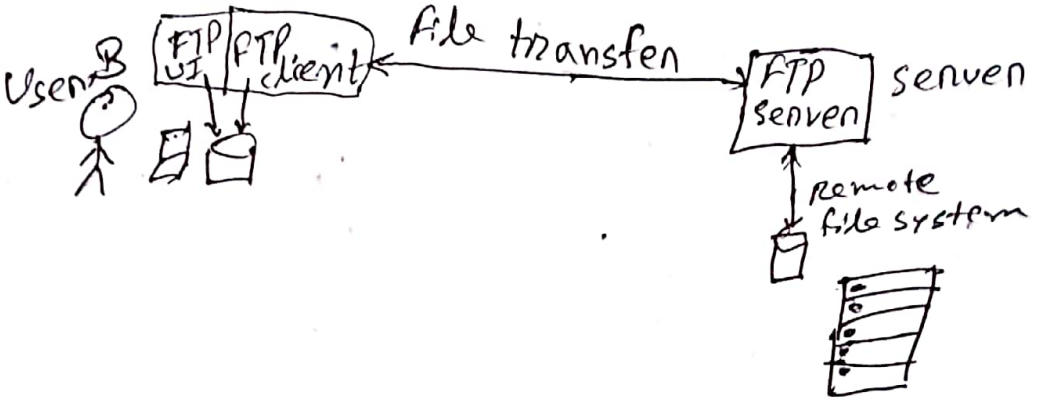
(2)

17201012

Answer to the Q. No. 1(b)

1TB

To transfer a file from A to B I'll choose File Transfer Protocol (FTP). FTP follows a client-server architecture. Client initiates connection at port 21. Then server opens data connection at port 20. Then the data can transfer from server to client.



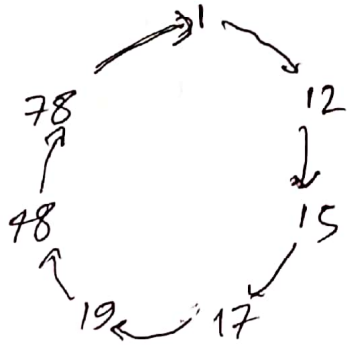
Here B is FTP client and A is FTP server. B contacts A at port 21 using TCP. B is authorized over control connections. When A receives file transfer command, A opens a 2nd TCP data connection at port 20 for file to client. The the 1TB file gets transfered from A to B. After transfering the file A closses the data connection.

This is the technology I have selected for data transmission.

17201012

Answer to the Q. No. 1(c)

A peer to peer network can be torrent. To search torrent we need to maintain index that is very complex due to peer churn. But if we use hash table we can get particular output for particular input. Hash output i.e. numerical output is easy to search and store than character value. ~~Key~~ Numerical key value is unique so there's no data redundancy. When we ~~search~~ search for a torrent it's name is hashed ~~then~~ we get the ~~key~~ key using which we can find the value associated with it. For this any peer can query database with a key and it is robust to peer churn.



Here hash key is 38. So the value of this key would be at the closest ID peer that is peer 48. So 48 is ~~to~~ now the assigned peer for key 38. So now peer 48 can give chunks to ~~the requester~~ whom made the request. These are the advantages of DHT is P2P network, ~~it is robust to peer churn.~~ Limitation of DHT is death of nodes ~~the~~ peer churn, though it can be handled via updating successor and predecessor history.

(9)

17201012

Answer to the Q.No:2(a)

Block chain technology is moving closer to friction free business environment. The formulation of my answer is given below with evidance.

i) Reducing information friction:

Uncertainty over the information needed to make business decisions often acts as a barrier to business. Blockchain has several protenties that reduce information friction, including the following:

1) Shared ledger: Block-chains shift the panadigm from information held by a single owner to a shared lifetime history of an asset on transaction.

2) Permission.

3) Cryptography

4) Consensus

ii) Easing interaction ~~&~~ friction:

Blockchain is particularly well-equiped to reduce ~~interact~~ interaction friction because it removes the barriers between participants in a transaction. Blockchain properties that reduce interaction friction include the following:

1) Shared ledger
2) State based communication
3) Peer to peer transaction
4) Consensus
5) Smart contracts

iii) Easing innovation friction:

Innovation friction is possibly the most ~~diff~~ difficult to overcome through technology alone, but blockchain can help in the following ways:

1) Eliminate the cost of complexity
2) Reduce costs and delays of regulatory process.
3) Expand opportunities.

(6)
17201012

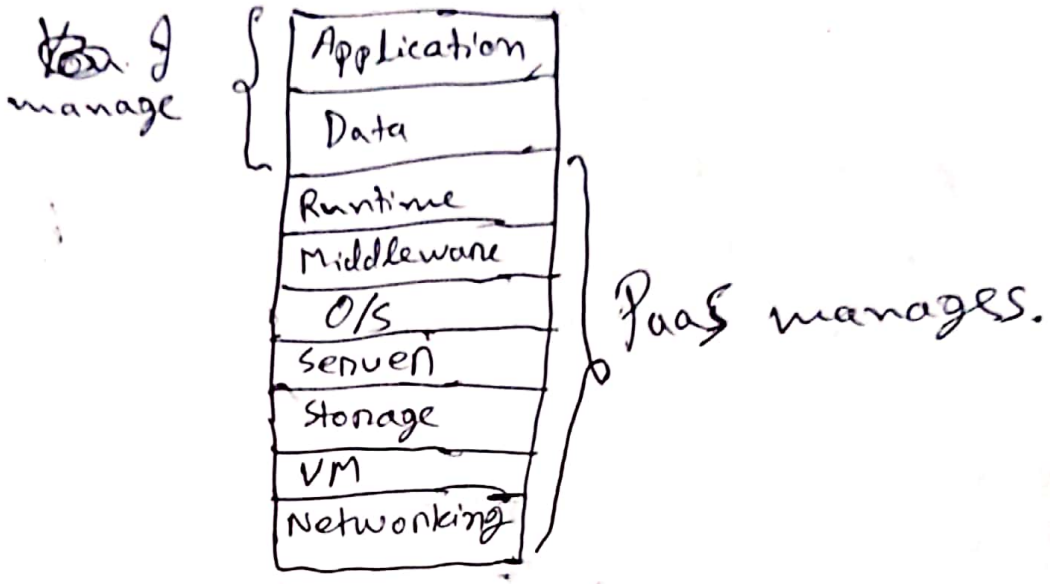
Answer to the Q. No. 2(b)

As I am an entrepreneur and want to build the service for small to medium sized business organization so I'll choose Platform as a Service in short PaaS to provide services. My reasonings are given below:

Paas is a mechanism for combining IaaS with an abstracted set of middleware services, software development and deployment tools that can be used to deploy applications on cloud or on-premises environment. It provides cloud platform for developing testing & managing applications. This service model enables users to deploy application without the need to acquire, manage & maintain architecture.

As I am an entrepreneur it'll be of great benefit to ~~have~~ use Paas as in Paas I just develop the service for business organization and all other things are maintained by it. For this I can provide more greater services.

P.T.O.

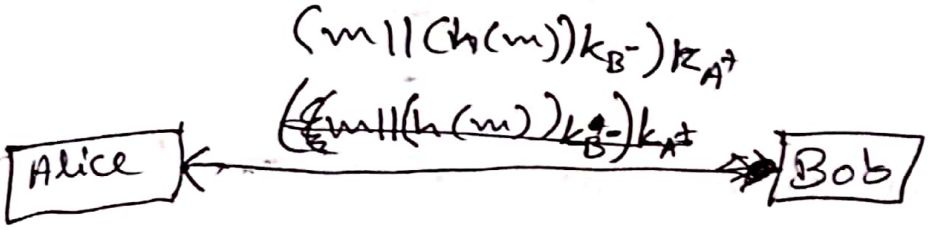


Thus using Paas is more beneficial for me as an entrepreneur.

(8)
1720102

Answer to the Q.No.3(a)

Design of a protocol that'll maintain authenticity, confidentiality and message integrity is given below.



Let assume Bob sends message to alice. So the process would be

→ The message is hashed and encrypted with Bob's private key (K_B). We hashed it due to it is less complex to encrypt hash as it is smaller in size.

→ Then the encrypted hashed message is concatenated with original message. For this Alice can hash the message and check if it maches already hashed message.

→ Then the concatenated message is encrypted with Alice's public key (K_A^+) so that only Alice can open it. Then Bob sends this to Alice.

What happens here is:

As it is encrypted with K_A^+ so only Alice can decrypt and read it ensuring confidentiality. Then Alice can decrypt the hash This also ensures integrity. Then Alice can decrypt the hashed message using Bob's public key (K_B^+) this ensures authenticity. Another thing Alice can also hash the message to match it with already hashed message this also ensures message integrity.

Answer to the Q. No. 3(b)

$q = 37$

$r = 41$

$m = 10$

$\therefore n = 1517$

$z = 1440$

$e = 1$

$d = 1$

$\therefore ed \% z = 1 \% 1440 = 1$

(10)

17201012

RSA:

$C = m^e \% n = 10 \% 1470 = 10$

∴ encrypted message, $C = 10$

Now to decrypte,

$m = C^d \% n = 10^1 \% 1470 = 10$

So we get the message to after decrypting this matches original message.

Answer to the Q No. 4(a)

Let base address = 172.16.0.0

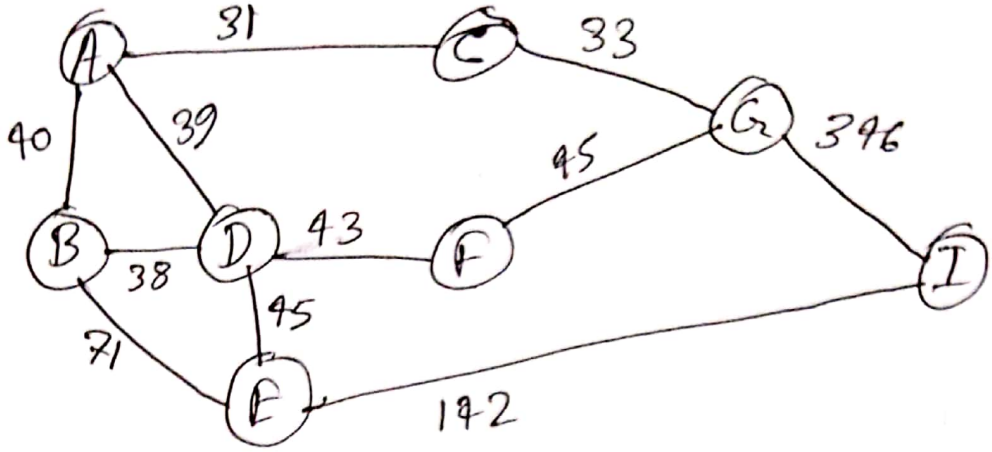
Name	Host req.	Network Address	Subnet mask	First host	Last host	Broadcast address
Branch users	1000 (10 bit host)	172.16.0.0/22	255.255.252.0	172.16.0.1	~~172.16.3.254~~ 172.16.3.254	172.16.3.255
Accounts	200 (8 bit host)	172.16.4.0/24	~~255.255.255.0~~ 255.255.255.0	172.16.4.1	172.16.4.254	172.16.4.255
Corporate	250 (8 bit host)	172.16.5.0/24	~~255.255.255.0~~ 255.255.255.0	172.16.5.1	172.16.5.254	~~172.~~ 172.16.5.255
Audit	100 (7 bit host)	172.16.6.0/25	255.255.255.128	172.16.6.1	172.16.6.126	172.16.6.127
Managers	70 (7 bit host)	172.16.6.128/25	255.255.255.128	172.16.6.129	~~172.16.6.254~~ 172.16.6.254	172.16.6.255

17201012

Answer to the Q. No. 9(b)

$x = 16 \times 9 = 40$; $z = 71 \times 2 = 142$

$y = 21 + 10 = 31$



P.T.O

STEP	N	D(B),P(B)	D(D),P(D)	D(C),P(C)	D(G),P(G)	D(F),P(F)	D(E),P(E)	D(H,I),P(I)
0	A	40, A	39, A	31, A	∞	∞	∞	∞
1	AC	40, A	39, A		64, C	∞	∞	∞
2	ACD	40, A			64, C	82, D	84, D	
3	ACDB				64, C	82, D	84, D	
4	ACDBG					82, D	84, D	410, G
5	ACDBGF						84, D	410, G
6	ACDBGFE							226, E

Shortest path : A → D → E → I

cost = 39 + 45 + 142 = 226

Ans.

—— 0 ——

12

17201012