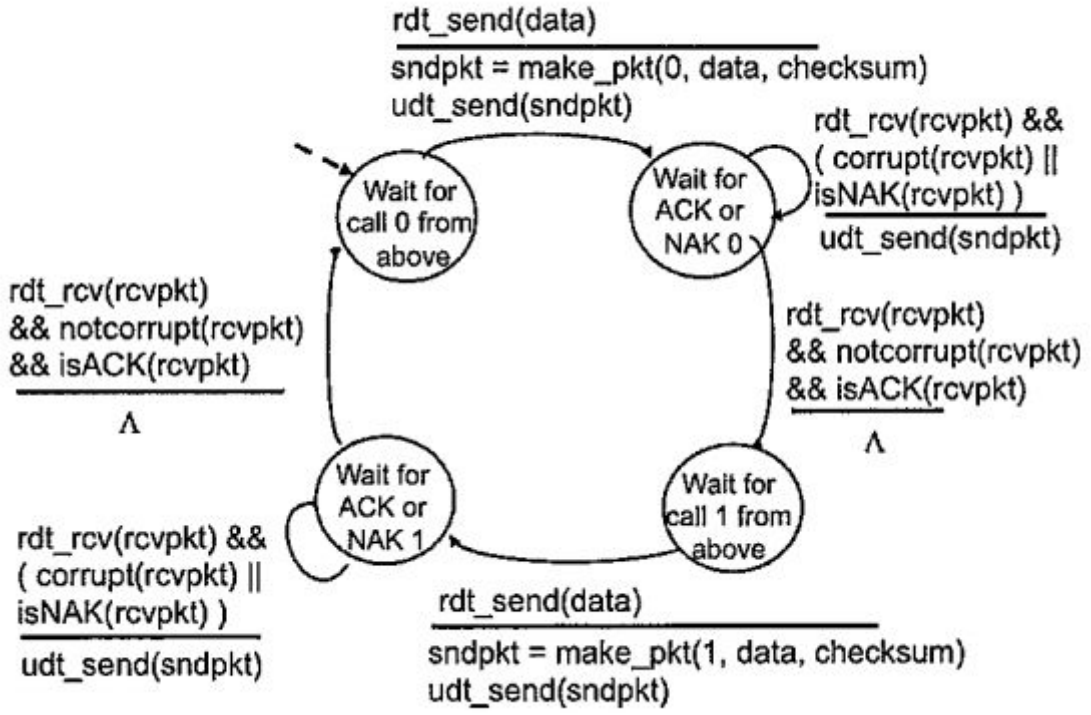
1. TCP vs UDP

1. Distinguish between UDP & TCP in terms of reliable data transfer, header size & connection overheads. [5 marks]
    a. Reliable data transfer
        i. TCP - Reliable, no loss, using ack system & selective repeat to error correct
        ii. UDP - Unreliable, no ack, provide error detection using checksum but no error recovery
    b. Header size
        i. TCP - At least 20 bytes. Requires sequence number & ack number. Has control flags, checksum, data offset & window size.
        ii. UDP - 8 bytes. Much smaller only source & dest port numbers, checksum & length of data.
    c. Connection overheads
        i. TCP - Larger overhead means slower connection. Error checking & correction introduce overhead but improve reliability
        ii. UDP - Smaller overhead increases speed. Less error handling improve speed but reduces reliability
2. Explain the difference between TCP & UDP under the headings: Connection, Function, Usage, Reliability, Packet Ordering, Speed of transfer, Data Flow control, Error Checking, Handshake & Examples (e.g. HTTP = TCP). [20 marks]
    a. Connection,
        i. TCP requires handshake to establish connection.
        ii. UDP does not.
    b. Function,
        i. TCP is all about reliability, it ensures a lossless connection and is used when packet integrity is important.
        ii. UDP's function is to send packet quickly without any correction for reliability.
    c. Usage,
        i. TCP - Email, http requests
        ii. UDP - Music/video streaming or interactive gaming
    d. Reliability,
        i. TCP - Reliable
        ii. UDP - Unreliable
    e. Packet Ordering,
        i. TCP - Packets ordered correctly using a selective repeat ack system

        ii. UDP - Packets can arrive in any order
    f. Speed of transfer,
        i. TCP - slower transfer due to overhead introduced by error handling
        ii. UDP - Fast transfer
    g. Data Flow control,
        i. TCP - Does flow control handles congestion.
        ii. UDP - No flow control option
    h. Error Checking,
        i. TCP - Does error checking. Erroneous packet are resent
        ii. UDP - Discards erroneous packets
    i. Handshake & Examples (e.g. HTTP = TCP).
        i. TCP - SYN, SYN-ACK, ACK
        ii. UDP - No handshake
3. Describe the functionality provided by UDP & TCP. [5 marks]
    a. The **transmission control protocol** (**TCP**) is used for applications in which **reliable** connections between hosts are necessary. TCP checks for transmission errors, lost packets, packets out of order, etc, and tries to automatically correct these without "bothering" the application program. It also does **flow control**, slowing transmission if it is too fast for the receiver.
    b. The **user datagram protocol** (**UDP**), is an unreliable transport protocol with no sessions or flow control and optional error checking. UDP just sends packets as soon as requested and forgets about them. It is faster than TCP, and is suitable for **isochronous** applications like **voice over IP** (**VOIP**) or streaming video where error correction is pointless.
4. Which one would you use for loop multimedia communications and why? [5 marks]
    a. UDP because multimedia (video/audio) can be lossy and still be understood, but also needs to be transmitted quickly
5. Would TCP or UDP be preferable for IP Telephony & IP Video Conferencing? Justify your answer. [5 marks]
    a. Same as above
6. A Web server using persistent connections is running on host C on port 80. It is receiving requests from both host A and B. Are all the requests being sent through the same socket on host C? If they are being passed through different sockets, do both the sockets have port 80? Discuss & Explain. [6 marks]
    a. For each persistent connection, the Web server creates a separate “connection socket”. Each connection socket is identified with a four-tuple: (source IP address, source port number, destination IP address, destination port number). When host C receives and IP

datagram, it examines these four fields in the datagram/segment to determine to which socket it should pass the payload of the TCP segment. Thus, the requests from A and B pass through different Sockets. The identifier for both of these sockets has 80 for the destination port; However, the identifiers for these sockets have different values for source IP addresses.

7. Draw the FSM for the receiver that corresponds to this sender's fsm.



8. If host A sends two packets to host B, the first with sequence number 65 and the second with sequence number 92, how much data is in the first segment? [3 marks]
    a. 65 bytes
9. If the first segment is lost and the second segment arrives, what will the ACK from B's acknowledgement number be? [3 marks]
    a. The ACK number will be 93
10. With the aid of an example, describe the TCP 'Fast Retransmit' algorithm and its advantages. [8 marks]
    a. TCP fast retransmit is a congestion control algorithm. For each connection, TCP maintains a congestion window, limiting the total number of unacknowledged packets that may be in transit end-to-end. This is somewhat analogous to TCP's sliding window used for flow control. TCP uses ‘slow start’ to manage the size of this window, starting small but growing with each received ACK

11. Why is TCP congestion control referred to as an additive-increase, multiplicative-decrease (AIMD) form of congestion control? [8 marks]
    a. This is because the window maintained to control congestion grows at a linear rate due to addition, but decrease by a multiplicative factor.

et $w(t)$ be the sending rate (e.g. the congestion window) during time slot t, a ($a > 0$) be the additive ncrease parameter, and b ($0 < b < 1$) be the multiplicative decrease factor.

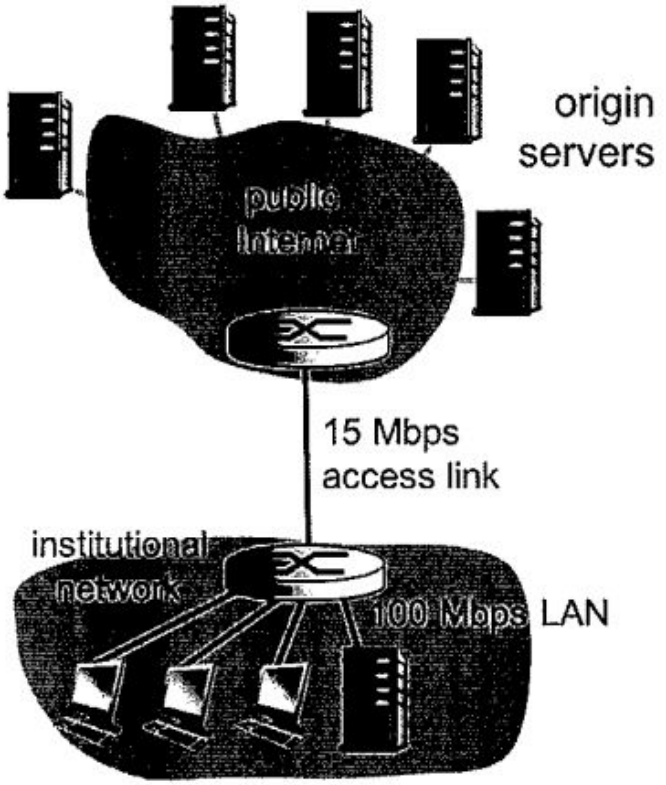
$$w(t+1) = \begin{cases} w(t) + a & \text{if congestion is not detected} \\ w(t) \times b & \text{if congestion is detected} \end{cases}$$

2. HTTP

1. Briefly explain the role of Hypertext Transfer Protocol (HTTP) in web communications. [5 marks]
    a. HTTP is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. As soon as a Web user opens their Web browser, the user is indirectly making use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet).
2. Why is HTTP 1.0 called a stateless protocol? [5 marks]
    a. HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it. This is the main reason that it is difficult to implement Web sites that react intelligently to user input. This shortcoming of HTTP is being addressed in a number of new technologies, notably cookies.
3. Describe how an e-commerce site can keep a purchase record of each of its customers using cookies. [10 marks]
    a. Cookies allow a Web site to store information on a user's machine and later retrieve it. This circumvents HTTP's statelessness problem, by storing persistent data locally. For example, if you make a purchase on Amazon.com, Amazon will store a cookie on your disk with a unique UserID. This means they can link your browsing to a User on their end and keep track off all your purchases. Cookies are stored as name value pairs on your machine and are access by your browser when you visit a website. If the correct name-value pairs are present they are sent to the webpage.
4. Consider the institutional network below, which is connected to the internet via a 15 Mbps access link. Suppose that the average object size is 960,000 bits and

that the average request rate from the institution's browsers to the origin servers is 15 requests per second. Also suppose that the amount of time it takes from when the router on the Internet side of the access link forwards an HTTP request until it receives the response is 2 seconds on average. Model the total average response time as the sum of the average access delay (that is, the delay from the internet router to the institution router) and the average Internet delay. For the average access delay, use $\Delta/(1-\Delta\beta)$, where Δ is the average time required to send an object over the access link and β is the arrival rate of objects to the access link.

5. Find the average response time. [6 marks]
    a. Time to transmit object of size L over a link of rate R is L/R960000/15000000 = 0.064 sec
        i. The traffic intensity on the link is given by $\beta\Delta$=(15 requests/sec)(.064 sec/request) = 0.96
        ii. Thus the avg access delay is (.064 sec)/(1 - .96) = 1.6 seconds
        iii. The total response time is therefore 1.6 sec + 2 sec = 3.6 sec



6.
7. Find the total response time if a cache is installed in the institutional LAN with a miss rate of 0.4. [6 marks]
    a. The traffic intensity on the access link is reduced by 60% since the 60% of the requests are satisfied within the institutional network. Thus the average access delay is (.064 sec)/[1 – (.4)(.96)] = 0.10389 seconds.

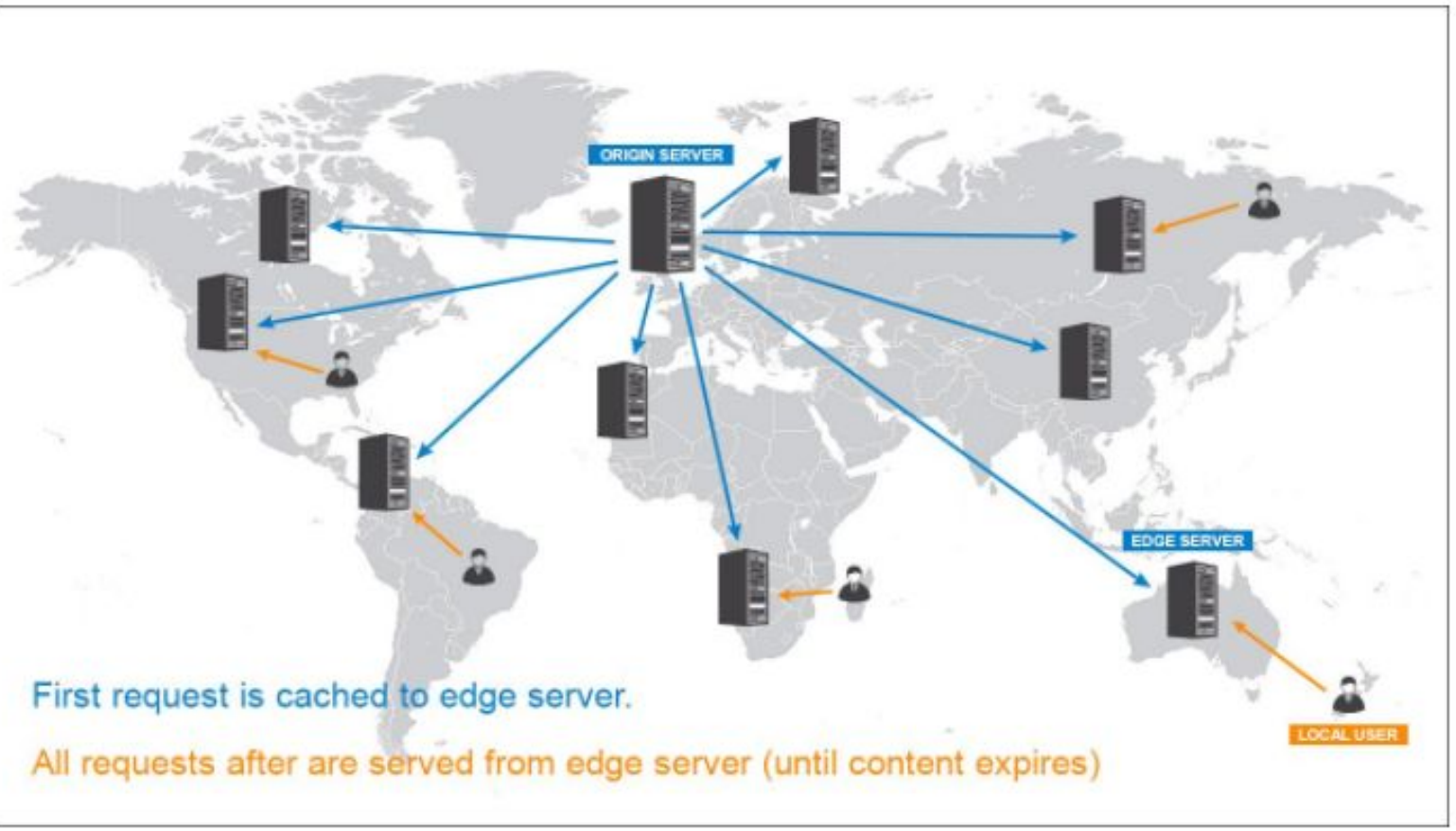
   b. The response time is approximately zero if the request is satisfied by the cache (which happens with probability .6); the average response time is .10389 sec.
      0.10389 sec + 2 sec = 2.10389 sec for cache misses (which happens 40% of the time). So the average response time is (.6)(0 sec) + (.4)(2.10389 sec) = 0.841556 seconds. Thus the average response time is reduced from 3.6 sec to 0.841556 sec

8. Consider what happens when a browser (i.e. a HTTP client), running in some user's host, requests the URL somesite.com/index.html. In order for the user's host to be able to send a HTTP request message to the Web server www.somesite.com. Explain the steps through which the IP address for such a hostname is obtained by the client. [12 marks]
9. What is a DNS? [1 mark]
   a. Domain Name Servers (DNS) are the Internet's equivalent of a phone book. They maintain a directory of domain names and translate them to Internet Protocol (IP) addresses.
      This is necessary because, although domain names are easy for people to remember, computers or machines, access websites based on IP addresses.
      Information from all the domain name servers across the Internet are gathered together and housed at the Central Registry. Host companies and Internet Service Providers interact with the Central Registry on a regular schedule to get updated DNS information.
      When you type in a web address, e.g., www.jimsbikes.com, your Internet Service Provider views the DNS associated with the domain name, translates it into a machine friendly IP address (for example 216.168.224.70 is the IP for jimsbikes.com) and directs your Internet connection to the correct website.
10. What protocol do DNS use? [2 marks]
   a. DNS queries consist of a single UDP request from the client followed by a single UDP reply from the server.
11. What would the implications be if all the DNS servers worldwide went offline at the same time? [2 marks]
   a. Any website that IP address isn’t stored in the local or systems local cache would be inaccessible by searching the url.
12. Describe in detail the operation and benefits provided by a Content Distribution Network (CDN). [10 marks]
   a. A content distribution network (CDN) is a geographically distributed network of proxy servers and their data centers. By setting up proxy

servers, that in essence act as a cache for a central server, we can reduce the latency for web access across the globe.

- Faster content load / response time in delivering content to end users.
- Availability and scalability, because CDNs can be integrated with cloud models
- Redundancy in content, thus minimizing errors and there is no need for additional expensive hardware
- Enhanced user experience with CDNs as they can handle peak time loads
- Data integrity and privacy concerns are addressed

CDN Diagram



13. What is the role of DNS in a Content Distribution Network (CDN)? [4 marks]
    a. DNS-based server redirecting is considered the most popular means of deploying CDNs. In CDN's the optimal server has to be selected depending on the user. Once it is, a server redirecting mechanism is implemented. Among all server redirecting mechanisms, DNS-based server redirecting is the most popular. Using the IP source address of a

DNS request, CDN's try to guess the proximity of the requester to each of many replicated content servers.

14. Does the DNS have to be modified to support the CDN? [3 marks]
    a. For a CDN to work, it needs to be the default inbound gateway for all incoming traffic. To make this happen, you'll need to modify your root domain DNS configurations (example.com) and all subdomains (www.example.com, img.example.com. The A records and CNAME record of the DNS are changed according to the CDN provider.
15. What information, if any, must a CDN provide to a DNS? [3 marks]
16. What is the role of a SIP registrar? [5 marks]
    a. A registrar is a server that accepts registrations from users and places these registrations, (which are essentially location information), in a database known as a Location Service. The process of registration associates a user with a particular location, (IP address); this association is known as a 'binding' in SIP.
17. How is the role of a SIP registrar different from that of a home agent in Mobile IP? [5 marks]
    a. In mobile IP, packets from the correspondent node are tunneled to the Mobile node through the home agent using the care-of-address obtained from the foreign agent.
18. How can a multimedia application recover from packet loss without the need for retransmission? [3 marks]
19. Describe in detail three methods discussed in lectures. [12 marks]
20. In BitTorrent, suppose Alice provides chunks to Bob throughout a 30-second interval. Will Bob necessarily return the favor and provide chunks to Alice in the same interval? [3 marks]
21. Consider Trudy joins the BitTorrent without possessing any chunks. Without any chunks, she cannot become a top-four uploader for any other peers, since she has nothing to upload. Then how will Trudy get her first chunk? [6 marks]

3. Security

1. Describe some of the components that comprise modern day block ciphers. In particular, describe with the aid of an example the Vignère Cipher. [8 marks]
    a. A block cipher is an encryption algorithm that operates on a fixed number of bits, and produces an unvarying transformation in accords with some symmetric key. The Vignere Cipher works as a series of Caeser Cyphers with a given keyword. THe letter of the keyword deciding the extent of the shifting.

b.

Plaintext:	ATTACKATDAWN
Key:	LEMONLEMONLE
Ciphertext:	LXFOPVEFRNHR

c. Using a Vignere square (below) you look up the column entry of the plain text and use the row entry of the keyword. That is your new letter.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

2. With the aid of an example, show why the electronic code book (ECB) mode is susceptible to substitution attacks. Describe the cipher block chaining (CBC) mode and how it can provide probabilistic encryption which overcomes the deterministic features of ECB mode. [10 marks]

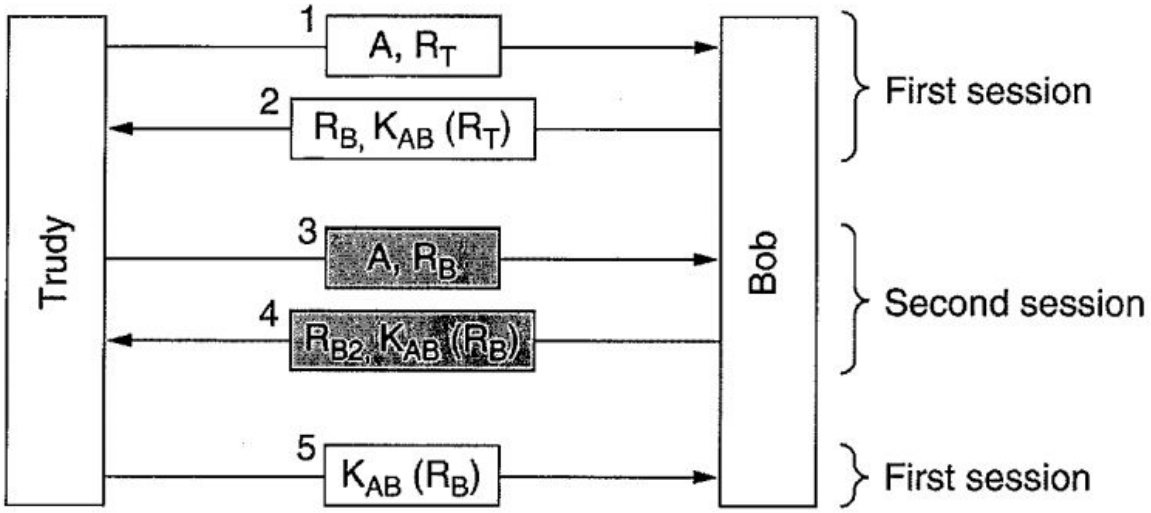
    a. Because in ECB each block is encrypted independently of other blocks, it allows a passive intruder to manipulate ciphertext blocks without the receiver noticing. For example, if someone can deduce the independent encryption mapping they can then substitute crucial fields to be in their favour, such as some altering the receiving account of a bank transfer
    b. CBC mode chains blocks of ciphertext together, each depending on the cipher before, this leads to less deterministic encryption. In CBC plaintext is XOR with the previous ciphertext before being encrypted. This way each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.
3. Define a cyclic group G. [2 marks]
    a. a cyclic group is a group that is generated by a single element. A group G is called cyclic if there exists an element g in G such that G = ⟨g⟩ = { gn | n is an integer }.
    b. A cyclic group G contain an element ‘a’ with maximum order i.e. ord(a) = |G|
4. What is the primitive element or generator of the group G? [2 marks]
    a. The element ‘a’ that has maximum order is a primitive element
5. Check if a=2 is a primitive element of $\mathbb{Z}^*_{11}$. [2 marks]
    a.
6. Is the group $\mathbb{Z}^*_{11}$ a cyclic group? [2 marks]
7. Compute the two public keys and the common key for the Diffie-Hellman key exchange (DHKE) scheme with parameters p=467, α=2, and a =228, b=57. [6 marks]
    a. A = g^a mod p = 2^228 mod 467 = 394
    b. B = g^b mod p = 2^57 mod 467 = 313
    c. keyA = B^a mod p = 313^228 mod 467 = 206
    d. keyB = A^b mod p = 394^57 mod 467 = 206
8. Show with the aid of an example how the DHKE scheme is vulnerable to man-in-the-middle (MITM) attacks. [6 marks]
    a. The Diffie-Hellman key exchange is vulnerable to a man-in-the-middle attack. In this attack, an opponent Carol intercepts Alice's public value and sends her own public value to Bob. When Bob transmits his public value, Carol substitutes it with her own and sends it to Alice. Carol and Alice thus agree on one shared key and Carol and Bob agree on another shared key. After this exchange, Carol simply decrypts any messages sent out by Alice or Bob, and then reads and possibly modifies them before re-encrypting with the appropriate key and transmitting them to the other party. This vulnerability is present because Diffie-Hellman key exchange does not authenticate the participants. Possible solutions include the use of digital signatures and other protocol variants.

9. The Diffie-Hellman key exchange is being used to establish a secret key between Alice and Bob. Alice sends Bob (227, 5, 82). Bob responds with (125). Alice's secret number, x, is 12, and Bob's secret number, y, is 3. Show how Alice and Bob compute the secret key. [15 marks]
    a. p=227, x =5, A =12 B=3
    b. x^A mod p = 5^12 mod 227 = 82
    c. x^B mod p = 5^3 mod 227 = 125
    d. 82^3 mod 227 = 212
    e. 125^12 mod 227 = 212
    f. Key = 212
10. If Alice and Bob have never met, share no secrets, and have not certificates they can nevertheless establish a shared secret key using the Diffie-Hellman algorithm. Explain why it is very hard to defend against the man in the middle attack. [15 marks]
    a. Difficult to detect
        i. If a man-in-the-middle attacker incepts the public key exchange, and replaces them with their own, it is almost indistinguishable from a genuine communication. Since there isn't any sort of identity verification of the two users. Alice and Bob have no way to distinguish each other from Carol.
    b. Insecure communication protocols HTTP over HTTPS (encrypted using SSL)
        i.
11. Alice used a transposition cipher to encrypt her messages to Bob. For added security, she encrypted the transposition cipher key using a substitution cipher key. Can Trudy decipher Alice's messages to Bob? Why or Why not? [15 marks]
    a. The answer to this question depends. If Trudy has access to the substitution and transposition keys, and knew which was done first, then she could decipher the messages. By simply using the substitution key to decrypt the substituted message, then use the transposition key to decrypt that. However if Trudy did not know the order which, or did not have access to the keys, she would not be able to decipher them.
12. Alice wants to communicate with Bob using public-key cryptography. She establishes a connection to someone she hopes is Bob. She asks him for his public key and he sends it to her in plaintext along with an X.509 certificate signed by the root CA. Alice already has the public key of the root CA. What steps does Alice carry out to verify that she is talking to Bob? [15 marks]
    a. Alice can use the public key of the root CA to decrypt the X.509 cert. Then using can verify that Bob's has the corresponding private key by sending a nonce. If the nonce returns correct, it is truly Bob.
13. Suppose that a system uses PKI based on a tree-structured hierarchy of CAs. Alice wants to communicate with Bob, and receives a certificate from Bob signed

by a CA X after establishing a communications channel with Bob. Suppose Alice has never heard of X. What steps does Alice take to verify that she is talking to Bob? [10 marks]

a. First Alice establishes a communication channel with X and asks X for a certificate to verify his public key. Suppose X provides a certificate signed by another CA Y. If Alice does not know Y, she repeats the above step with Y. Alice continues to do this, until she receives a certificate verifying the public key of a CA Z signed by A and Alice knows A's public key. This may continue until a root is reached, that is, A is the root. After this Alice verifies the public...

14. Change one message in the exchange below in a minor way to make it resistant to the reflection attack. Explain why this change works. [5 marks]



a. TO protect against a reflection attack we want to add an identifier with the original nonce that Trudy sends to Bob as a challenge. If we can link the nonce (and subsequent encryption of said nonce) with Trudy's identification then we can ensure that Bob is responding to Trudy's nonce and not getting a reflected answer from somewhere else.
b. We can change the first challenge trudy issues to Bob by sending a ID that must be encrypted with the nonce

15. Describe in detail the Handshake in the secure sockets layer (SSL) protocol. [4 marks]

a. We will break the handshake up into 3 main phases - Hello, Certificate Exchange and Key Exchange.
    i. Hello - The handshake begins with the client sending a ClientHello message. This contains all the information the server needs in order to connect to the client via SSL, including the various cipher suites and maximum SSL version that it supports. The server responds with a ServerHello, which contains similar information

required by the client, including a decision based on the client's preferences about which cipher suite and version of SSL will be used.

ii. Certificate Exchange - Now that contact has been established, the server has to prove its identity to the client. This is achieved using its SSL certificate, which is a very tiny bit like its passport. An SSL certificate contains various pieces of data, including the name of the owner, the property (eg. domain) it is attached to, the certificate's public key, the digital signature and information about the certificate's validity dates. The client checks that it either implicitly trusts the certificate, or that it is verified and trusted by one of several Certificate Authorities (CAs) that it also implicitly trusts. Note that the server is also allowed to require a certificate to prove the client's identity, but this typically only happens in very sensitive applications.

iii. Key Exchange - The encryption of the actual message data exchanged by the client and server will be done using a symmetric algorithm, the exact nature of which was already agreed during the Hello phase. A symmetric algorithm uses a single key for both encryption and decryption, in contrast to asymmetric algorithms that require a public/private key pair. Both parties need to agree on this single, symmetric key, a process that is accomplished securely using asymmetric encryption and the server's public/private keys.

16. When we talk about authentication in SSL, explain if we mean *message authentication* or *entity authentication*. [4 marks]
    a. Entity authentication. SSL provides a secure tunnel for which to send messages but it gives no assurance that the identity of the sender/recipient is correct. We must use digital certificates to ensure entity authentication. This is opposed to message authentication which is used to check the integrity of data sent across an insecure channel. Usually with a MAC.
17. What is the purpose of the random nonces in the SSL handshake? [4 marks]

a. Random nonces secure the channel from replay attacks, since a nonce must be used, and the nonce is always random with no duplicates, then a replay attack is prevented.

> A normal nonce is used to avoid replay attacks which involve using an expired response to gain privileges. The server provides the client with a nonce (Number used ONCE) which the client is forced to use to hash its response, the server then hashes the response it expects with the nonce it provided and if the hash of the client matches the hash of the server then the server can verify that the request is valid and fresh. This is all it verifies; *valid and fresh*.

18. In what way does a hash provide a better message integrity check than a checksum (e.g. a CRC)? [4 marks]

a. A Hash provides better message integrity because it has less collisions then an Internet checksum. A collision means there is more than one way to produce the same sum. A great hash function aims to reduce the occurrence of collisions.
b. Let H() be a hash function. Let x and y be two differing messages.
c. H(x) = H(y) would be a collision.

19. Explain whether you can 'decrypt' a hash of a message to get the original message. [4 marks]
    a. No. A hash may not be reversed, which means it cannot be decrypted. By design a hash algorithm has no inverse, there is no way to get the original message from the hash. A hash is 1-way trapdoor function.
20. Show with the aid of an example how Alice and Bob can exchange a 'Signed and Enveloped Message' using digital signatures. [12 marks]
    a. First a digital signature is developed using some function such as fig 1:

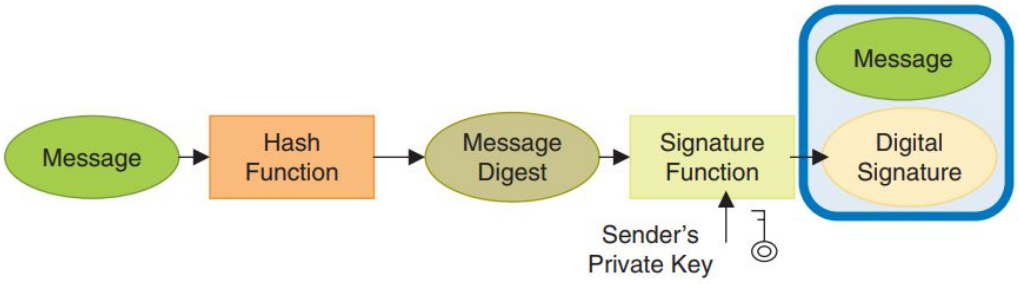


Fig. 1 Creating a digital signature

    b.
    c. Creating a digital envelope is then done by encrypting the message and also encrypting the key used to encrypt that message with a public key. See fig 3

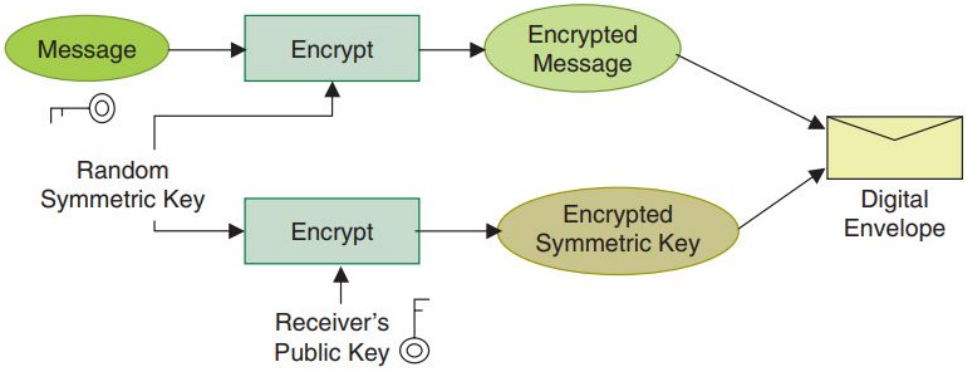


Fig. 3 Creating a digital envelope

    d.
    e. The two can then be combined by encrypting the message/signature combine and placing it in a digital envelope. Fig 5 shows this.

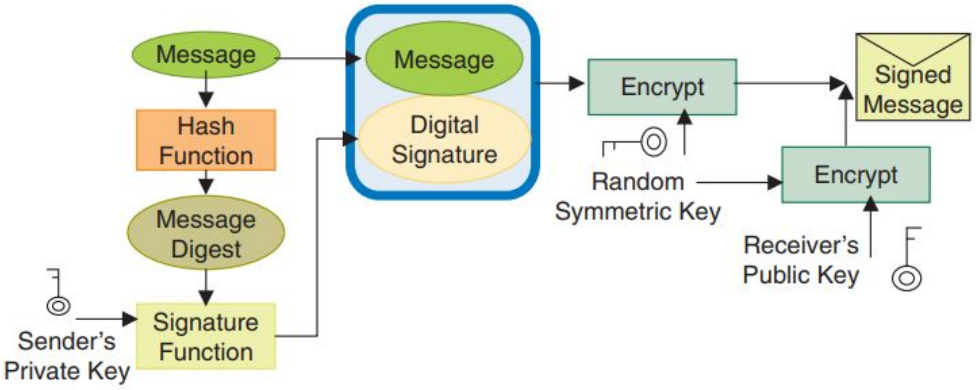
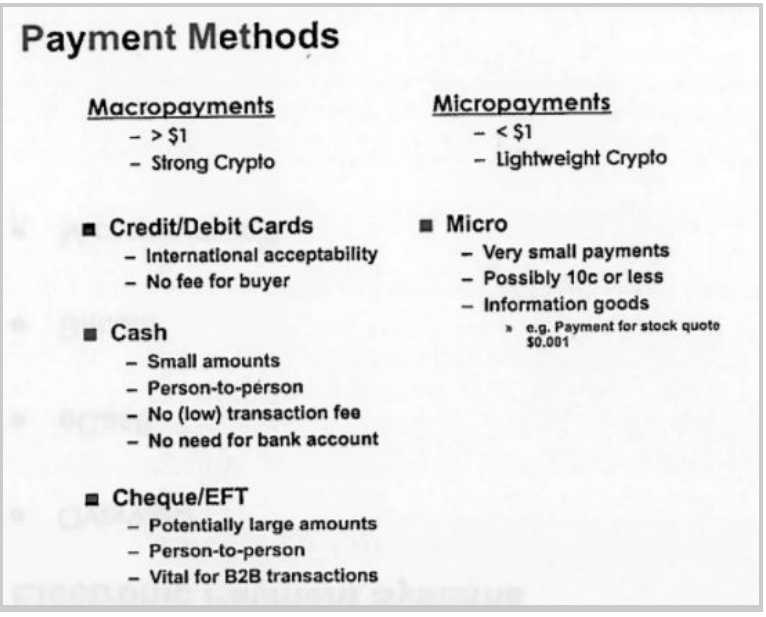


Fig. 5 Creating a digital envelope carrying a signed message

f.

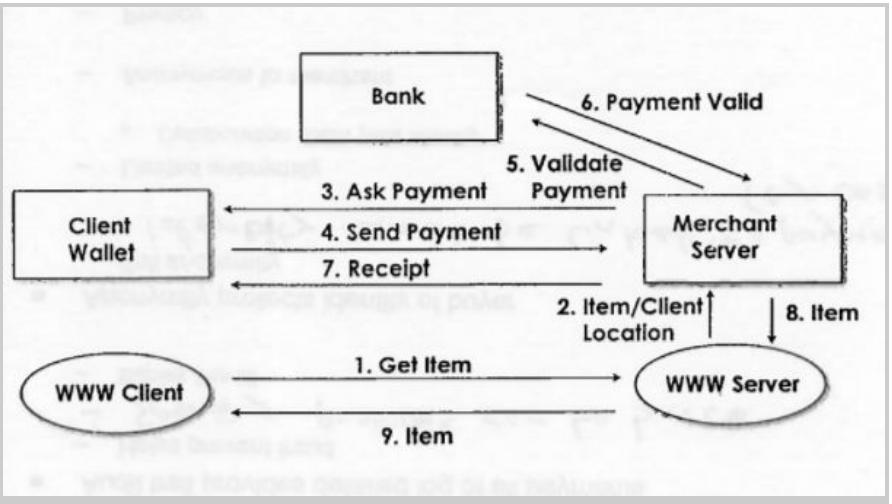
21. Compare and contrast Macropayment and Micropayment systems giving examples of each. [6 marks]

a.



b. MacroPayment system - e.g. Buying clothes online with credit card

c.



    d. MicroPayment system - e.g. buying ask to a pdf for .005c with eCash i.e/ Bitcoin it is lightweight and design for quick authentication & authorization. Sys example = PayWord

22. Explain what you understand by the phrase 'Proof-of-Work' in the context of the Bitcoin electronic cash scheme. [6 marks]
    a. The PoW system combines 2 main ideas, make it difficult for users to verify transactions in a system, and reward them for doing so. People part of the network hear about unverified transactions an add them to a queue for verification. Say David checks his copy of blockchain and sees that all the transactions are valid, as part of validation he would have to complete a computationally diffcult problem, usually finding a nonce that will hash (with the list of transactions) to return a number with many leading zeroes. This is Proof-Of-Work.
23. Differentiate between Symmetric and Asymmetric key cryptosystems giving advantages and disadvantages of each approach. Show how symmetric ciphers can be used in conjunction with asymmetric ciphers for secure session key exchange and fast bulk encryption. [15 marks]
    a. Symmetric cryptosystems use a single shared key that is used to encrypt and decrypt messages. This key needs to be secret, as if it is discovered the messages can be intercepted and read.
        i. Symmetric cryptosystems have the advantage of simplicity.
        ii. They have problems surrounding key distribution and keeping the key secret.
        iii. Symmetric system are generally faster than asymmetric ones.
        iv. Key are simple to generate.
    b. Asymmetric cryptosystems use 2 keys, a public and private key. Someone’s public key is used to encrypt messages sent to them, but only their private key can decrypt those message.
        i. Asymmetric cryptosystems are more complicated, key need to have certain characteristics to be viable
        ii. They solve the problem of key distribution as every has access to the public key and no one access to the private key
        iii. Generally slower as keys are more complex to generate.
    c. The two can be combined, first we generate asymmetric keys and encrypt our message with them, then we encrypt those keys with some secret key in order to securely exchange them. Also because symmetric key systems are much faster, they they are used for bulk data. The symmetric secret keys can be distributed using an asymmetric system, or can be generated periodically.
24. Encrypt the message "THIS IS AN EXERCISE" using a shift cipher with a key of 20. Explain with an aid of an example why such ciphers can be easily broken. [10 marks]

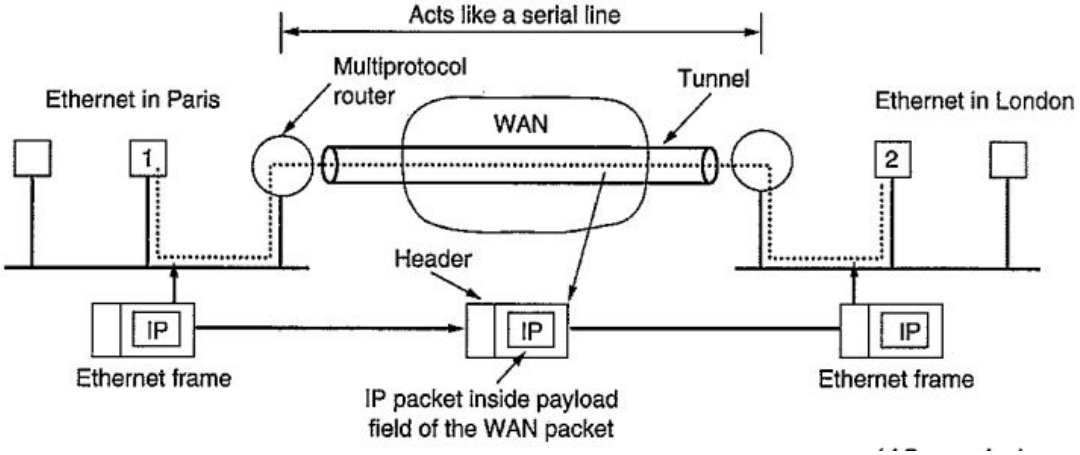
a. nbcm cm uh yrylwcmy
b. They can be easily broken by brute force guessing the key that was used. Also information about the message such as length is preserved/ We can examine common letters & common letter coupling to find letter like ‘e’ and ‘th’. Once we do that we know the shifting key and it is easily broken.

25. Using RSA, choose p=3 and q=11, and encode the word 'hello'. Apply the decryption algorithm to the encrypted version to recover the original plaintext message. [15 marks]
    a. N =P * q = 33
    b. o(N) = (p-1) * (q-1) = 20
    c. E =3 (choose number less than N with no common factors with o(N))
    d. D = (3^-1)mod20 = 7 our key is 7
    e. Hello = 8 5 12 12 15 (each bocket of plaintext given numerical value)
    f. ciphertextBlock = (plaintextBlock)^e mod n = 8^3 mod 33 = 17
    g. 5^3 mod 33 = 26
    h. 12^3 mod 33 = 12
    i. 15^3 mod 33 = 9
    j. Decryption = (cipherTextBlock)^d mod n =
    k. ((17^7) mod 33) = 8
    l. ((26^7) mod 33) = 5
    m. ((12^7) mod 33) = 12
    n. ((15^7) mod 33) = 15
26. Consider RSA with p=7 and q=13:
    a. i. What are n and ϕ(n)? [3 marks]
        i. 91 and 72 respectively
    b. ii. Let e be 5. Why is this an acceptable choice for e? [3 marks]
        i. Yes, it is lower than n and has no common factors with o(n)
    c. iii. Find d such that $e*d \equiv 1 (\mathrm{mod} \phi(n))$. [3 marks]
        i. (5^-1) mod 72 = 29
    d. iv. Encrypt the message m=9 using the key (e,n). [3 marks]
        i. m=13, ‘=’ = 27, 9=9
        ii. ((13^5) mod 91) = 13
        iii. ((27^5) mod 91) = 27
        iv. ((9) mod 91) = 81
27. To show that you understand the security of hte RSA algorithm, find d if you know that e=17 and n=187. [15 marks]
28. Trudy's RSA keys are as follows: n_t=33,d_t=3, e_t=7. Trudy finds out that Bob's public key is n_b=33, e_b=3. How can Trudy use this information to read encrypted messages from Bob? Explain with the aid of a worked example. [15 marks]
29. Summarize the key differences in the services provided by the Authentication Header (AH) protocol and the Encapsulation Security Payload (ESP) protocol in IPsec. [10 marks]

30. What are the differences between message confidentiality and message integriy? [4 marks]
31. Can you have one without the other? [2 marks]
32. Show how message integrity can be achieved using symmetric an asymmetric key cryptographic techniques. [6 marks]
33. In the Needhan-Schroder authentication protocol, Alice generates two challenges R_A & R_{A2}. This seems like overkill. Would one not have done the job? Justify your answer by showing the protocol exchanges between Alice, the Key Distribution Centre (KDC) and Bob. [15 marks]
34. Summarize the key differences in the services provided by the Authentication Header (AH) protocol and the Encapsulation Securtiy Payload (ESP) protocol in IPsec. [8 marks]
35. Explain with the aid of an example how Alice and Bob can mutually authenticate each other using a hashed message authentication protocol (HMAC). Give one advantage of HMACs over using RSA to sign SHA-1 hashes. [10 marks]

4. IP

1. Briefly describe the various datalink and network layer protocols used in transporting IP datagrams from the source to destination machines in the figure below. [12 marks]



a. The purpose of the two layer is as follows:

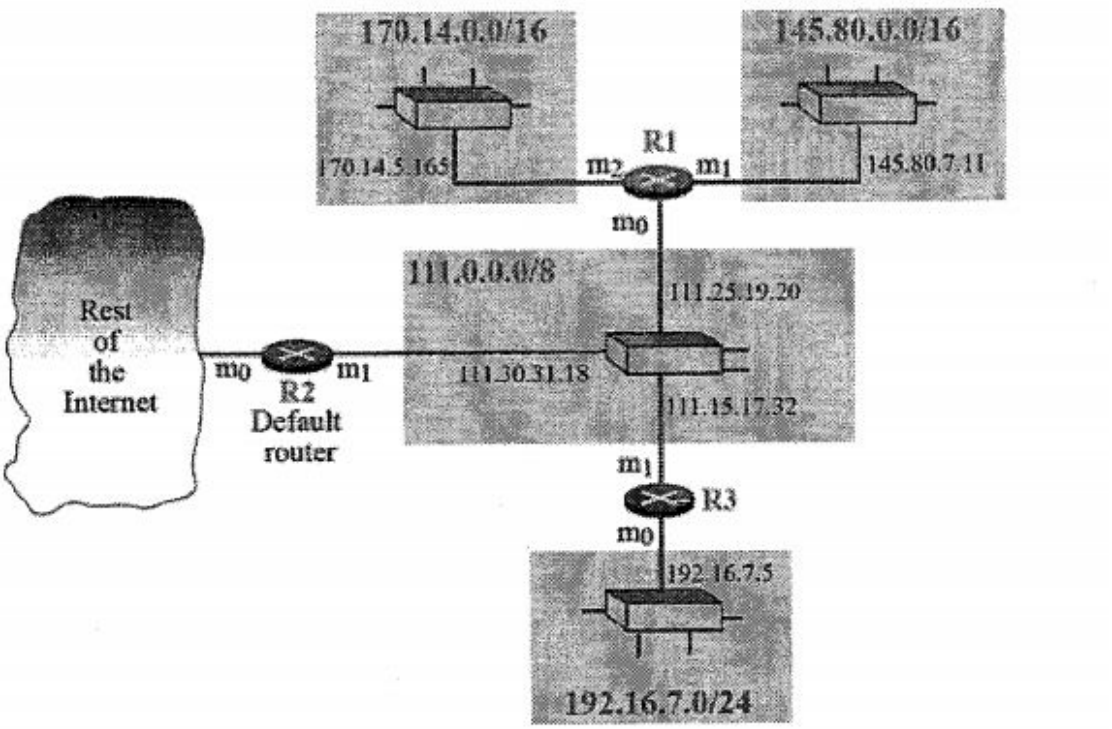
3. Network	Packet	Structuring and managing a multi-node network, including addressing, routingand traffic control
2. Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer

b.

2. Explain the meaning of the term 'IP address class' and why these classes were created. List the number of networks, hosts and the default mask in each of the first three classes. Explain in detail how 'classless' addressing overcomes some of the restrictions of classful addressing. [10 marks]
3. Distinguish between Classful and Classless addressing in IP networks highlighting the advantages and disadvantages of each approach. [8 marks]
4. Describe the 'slash notation' used in Classless Inter Domain Routing (CIDR). If one address in a block is 202.44.82.16 and the subnet mask is 255.255.255.192, find the network prefix, first address and the last address. [10 marks]
5. If one address in a block is 167.199.170.82/27, find the number of adresses in the network, the first address and the last address. [5 marks]
6. An organization is granted the block 130.56.0.0/16. The administrator wants to create 1024 subnets. Find: i. The number of addresses in each subnet. [3 marks] ii. The subnet prefix. [3 marks] iii. The first and last address of the first subnet. [3 marks] iv. The first and last address of the last subnet. [3 marks]
7. An organization is granted the block 211.17.180.0/24. The administrator wants to create 32 subnets. Find: i. The number of addresses in each subnet. [5 marks] ii. The subnet mask. [5 marks] iii. The first and last address of the first subnet. [5 marks] iv. The first and last address of the last subnet. [5 marks]
8. Is it possible for an organization's Web server and mail server to have exactly the same alias for a hostname (e.g. foo.com)? What would be the type of RR that contains the hostname for the mail server? [8 marks]
9. Describe with the aid of an example the concept of Multiprotocol Label Switching (MPLS). [6 marks]
10. What the specific support is there for MPLS in IPv6? [4 marks]
11. Compare and contrast the IPv4 and IPv6 header fields. [7 marks]
12. Why is the *Protocol* field used in the IPv4 header not present in the fixed IPv6 header? [3 marks]

13. Specify the routing table for the router R3 in the figure below. [15 marks]

(15 m



14. The routing table for a router R1 is provided in the table below. You are required to draw the topology of the resulting network. Explain any assumptions that you may have had to make. [15 marks]

Mask	*Network Address*	*Next-Hop Address*	*Interface Number*
/26	140.6.12.64	180.14.2.5	m2
/24	130.4.8.0	190.17.6.2	m1
/16	110.70.0.0	----------	m0
/16	180.14.0.0	----------	m2
/16	190.17.0.0	----------	m1
Default	Default	110.70.4.6	m0

15. List the entities of Mobile IP and describe the process of data transfer from a mobile node to a fixed node and vice versa. [10 marks]
16. Why and where is encapsulation needed? [5 marks]
17. Name the inefficiencies of Mobile IP regarding data forwarding from a correspondent node to a mobile node. [5 marks]

18. What are the optimizations and what additional problems do they cause? [10 marks]
19. What are the general problems of Mobile IP regarding security? [5 marks]
20. Why is routing in multi-hop ad-hoc networks complicated, and what are the special challenges? [5 marks]
21. How does the Dynamic Source Routing (DSR) protocol handle routing? [5 marks]
22. What is the motivation behind DSR compared to other routing algorithms from fixed networks? [5 marks]

5. Medium Access Control

1. Describe the various Medium Access Control (MAC) schemes employed in cellular networks, highlighting their advantages and disadvantages. [12 marks]
2. In a typical mobile phone system with hexagonal cells, it is forbidden to reuse a frequency band in an adjacent cell. If 840 frequencies are available, how many can be used in a given cell? [4 marks]
3. Describe in detail the steps involved during a GSM 'Mobile Terminated Call', e.g. when a node in the PSTN makes a call to roaming mobile node. [12 marks]
4. Explain why there is a need for a 'handover' to take place in mobile networks. [5 marks]
5. Identifying the network entities involved in each case, what are the various types of handover that can occur in GSM networks?[5 marks]
6. With the aid of an example, outline the inefficiencies of Mobile IP regarding data forwarding from a correspondent node to a mobile node. [6 marks]
7. What are the optimizations and what additional problems do they cause? [6 marks]
8. Describe in detail the four fundamental channel-access schemes used in a telecommunications system hightlighting their strengths and weaknesses. Give an example of an application of each scheme (or a combination of them). [16 marks]
9. With the aid of a diagram, describe the main entities that comprise a 2G (GSM) and 3G (UMTS) mobile network architecture. List the purpose and functions of each component and the interactions between them. [15 marks]
10. Explain what is meant by the 'Hidden Terminal' & 'Exposed Terminal' problems, giving an example of each. [8 marks]
11. Describe in detail a multiple access method used in 802.11 networks to avoid collisions. [7 marks]

12. Explain why when a mobile user crosses the boundary from one cell to another, the current call is abruptly terminated, even though all transmitters and recievers are functioning perfectly. [4 marks]
13. Outline the key distinguishing features of a Local Area Network (LAN). Describe the various 'pure' and 'hybrid' topologies in use today giving advantages and disadvantages of each. [15 marks]
14. Briefly explain the operation of Ethernet (802.3), Fast Ethernet (802.3u) and Gigabit Ethernet (802.3z) with particular emphasis on the slot-time, minimum frame size, netowork length and their interdependancies. [20 marks]
15. Explain why there is no need for CSMA/CD in a full-duplex Ethernet LAN? [5 marks]
16. What are the advantages of dividing a LAN with switches? [5 marks]
17. Show how a switch is able to make use of MAC layer addressing to quickly switch packets from one collision domain to another. [5 marks]