Instructions: Answer FIVE Questions only. Each carries 20 marks.

Question 1 (20 marks)
Answer FOUR parts only. Each carries 5 marks:

i) Outline the structure of computer names used by DNS.

DNS uses a hierarchical naming scheme that forms an inverted tree when viewed from the root. The most significant part of a domain name is on the right which identifies the top level domain. The host name is the leftmost part. Intermediate parts identify subdomains.

e.g. www.yale.edu
www.itcarlow.ie
venus.cs.tcd.ie

Top level Domains

.com, .edu, .int, .gov, .mil, .org, .arpa, .country code

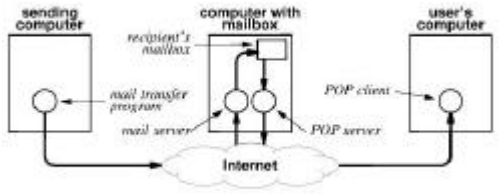
Naming authorities only look after names under the top level domains - organizations responsible for how they partition that. Some countries do partition top level domains

e.g. .ac.uk or .co.uk

Naming follows organizational boundaries not physical networks

ii) Describe the main features of the Post Office Protocol (POP)

POP3 (Post Office Protocol 3 .. defined in RFC 1225) is a simple protocol used for retrieving mail from a remote mailbox. The computer maintaining the mailbox must run an additional server that supports the POP3 protocol. A user runs e-mail software that interacts with the POP server to retrieve e-mail messages from the server.



Note that the SMTP server and POP server communicate across the Internet but use different protocols. Also the SMTP server accepts messages from an arbitrary server, whereas the POP server will only allow an authenticated user to access their mailbox.

POP is particularly popular with those users with dial-up accounts.

iii) What causes network congestion and outline 2 solutions for it.

Congestion is a fundamental problem in packet switching systems caused when sending stations swamp bottleneck with packets. Bottleneck queue builds up causing further congestion and possibly packet loss. Solution A involves getting the bottleneck device to send back a control message to sending stations advising them to reduce output. Solution B involves sending stations using packet loss as an estimate of congestion and reducing output accordingly – based on the premise that most packet loss on modern networks is caused by congestion.

iv) Distinguish between Anonymous vs non-Anonymous FTP

There are two types of FTP connections available on the Internet:
ii)anonymous
iii)non-anonymous

The most widely used type is anonymous FTP. If a file is stored in an anonymous FTP directory virtually anyone with Internet access and an FTP program of some sort, even a web browser, can download the file.

Uploading, on the other hand, is not usually possible with anonymous FTP. Anonymous FTP, therefore, is used primarily to give the Internet public download access to a particular directory of files. Anyone can download files from the directory, but only the "owner" of directory can upload to the directory.

When you connect to any FTP directory, the host system asks for your username and password before allowing you access to the directory (this process is done behind the scenes when you use a web browser to access an FTP directory). With an anonymous FTP directory, the username is always "anonymous" and the password is always the user's e-mail address. Non-anonymous FTP, on the other hand, requires a unique username and password for the FTP directory in question.

v) Describe how the Address Resolution Protocol (ARP) operates.

ARP used to by workstation to get hardware address of machine on same network segment. Machine A has the IP address of Machine B but needs its hardware address to communicate. Uses ARP – broadcasts ARP packet to all stations. Packet contains IP address of the remote machine, which replies with its hardware address.

Question 2 (20 marks)
Answer all parts

i) Describe the main features of the IP protocol. (3 marks)

IP (defined in RFC 791) is the core protocol of the TCP/IP suite. It provides a connectionless, unreliable data delivery service. All TCP and UDP data are transmitted as IP datagrams. The main functions of the IP protocol include addressing, packet routing, packet fragmentation and reassembly.

ii) Explain the five classes of IP address (5 marks)

There are five classes of IP address and they are distinguished both by the number of octets used for the network id and the address range of the first octet.

	8 bits	8 bits	8 bits	8 bits
Class A	0 Net id		Host	
Class B	10 Net	id	Host	
Class C	110	Net id		Host
Class D	1110	Multicast		address
Class E	1111		Reserved	

Classes A, B and C are called the primary classes because they are used for host addresses.
Class D is used for multicasting. Whereas a broadcast is directed to all hosts on the network, a multicast is sent only to the members of the multicast group.

iii) There are five reserved IP addresses. What are these and what are they used for? (5 marks)

Some addresses are reserved and cannot be used to assign to hosts.

Network Address

- Host address is 0.

Directed Broadcast Address

- Host address is all 1s.
- Single packet traverses the internet to the destination network. The packet is then delivered to all hosts on the network.

Limited broadcast address

- IP address consisting of all 1s
- A broadcast on the local network.

This computer address

•IP address consisting of all 0s
•For computers that do not have an IP address yet.

Loopback address
•Class A network address is 127
•Used for testing

iv) **A company with a network address of 156.157.0.0 wants to segment the network into 18 different subnets? What subnet mask is needed and how many hosts per subnet could be supported?** **(2 marks)**
255.255.248.0, 2^11-2

v) **What subnet mask is needed for a class C network divided into 5 different subnets and how many hosts per subnet could be supported?** **(2 marks)**
255.255.255.224, 2^5-2

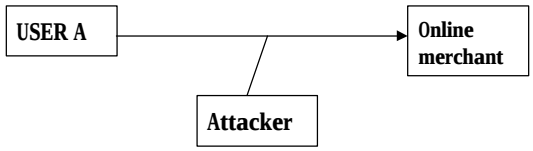
vi) **What subnet mask is needed for a class B network divided into 10 different subnets and how many hosts per subnet could be supported?** **(2 marks)**
255.255.255.240, 2^12-2

vii) **How many bits does IPv6 use for network addresses?** **(1 mark)**

Question 3 (20 marks)
Answer all parts

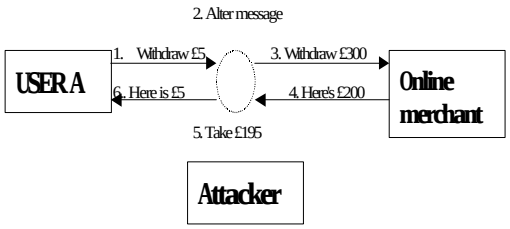
i) **Outline four methods of attack on an e-commerce system.** **(4 marks)**

Methods of attack

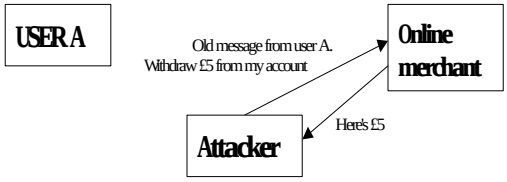


eavesdropping (easy on broadcast networks)
copies of messages obtained without authority
how? - listen to network traffic
OR set machine address to match others

masquerading (at the human or machine level)
send or receive messages using a stolen identity, token or access capability
attacker pretends to be another valid user, merchant or even bank
How? Steal passwords, PINs, account #, identity details etc. by eavesdropping
Use stolen details to withdraw funds or make purchases



message tampering (easy for store and forward, hard with broadcast networks)
Capture a message and alter it
Send altered message to original recipient
Includes substitution, deletion, new message construction.
interrupt communications channel (denial of service)

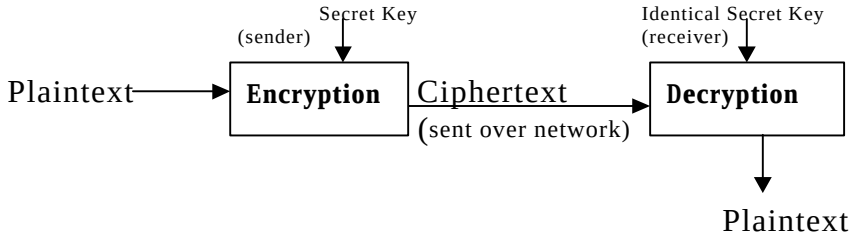


replay
Send recorded message (eavesdropped) again at a later time
e.g. replay a request to withdraw money from a bank

ii) Distinguish fully between Symmetric and Asymmetric Cryptosystems. (8 marks)

2 types of Cryptosystem:
1. *Symmetric*: Identical keys used to encrypt and decrypt (secret key algorithm)
2. *Asymmetric*: Two different keys used to encrypt and decrypt (public-key algorithm)

Symmetric Cryptosystems
Identical keys to encrypt and decrypt
The key must be kept a secret (secret key)
Both sender and receiver must know key
Examples: DES, Triple DES, RC5



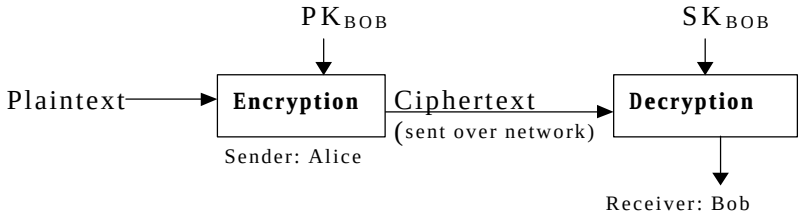
Notation: $E_K(P)=C$ $D_K(C)=P$

Asymmetric Cryptography
- Big problem with symmetric cryptography: Key management problem
- Solution: Asymmetric cryptography (public-key cryptography)
- Different keys used to encrypt and decrypt

Each user has 2 keys
- Public key: Made available to everyone
- Private key: Kept a secret by the user

Anyone with the public key can encrypt a message but not decrypt it.
Only the private key can decrypt.

Example
Alice sends a message to Bob so Alice gets Bob's public key. Alice encrypts message with Bob's public key and sends it. Only Bob's private key can decrypt it



Asymmetric vs Symmetric
Asymmetric offer:
+ Increased security
private keys are never transmitted over the network
- Much slower than symmetric cryptosystems

iii) Explain what is meant by a digital signature and identify how it is used? (4 marks)
If users are assigned public/private key pairs, then applying the private key to a message is tantamount to SIGNING the message
- only holder of the private key could have originated the message
- message integrity is assured - but SLOW
- anyone can read/verify the message

Same effect can be got by signing the message digest alone:
- much faster
- message sent in clear

iv) Explain what is meant by a message digest and identify how it is used? (4 marks)
Functions that are applied to a (long) message to produce a unique (short) "fingerprint" of the message
Properties:
Given a message M, it is easy to compute the digest D.
Given D, it is hard to compute M
Given M, it is hard to find another message M1 that will produce the same digest D.
Uses:
Used primarily as a message integrity checker. Can determine whether message has been altered in transit. Message is sent in clear, digest is encrypted and sent.

Question 4 (20 marks)
Answer all parts

i) What is a network's topology? (1 mark)
General shape of the network

ii) Distinguish between the following network topologies: (6 marks)

a) Star
DIAGRAM … star shaped. Computers connect to central hub.
b) Bus
DIAGRAM … computers connect to shared cable.
c) Ring
DIAGRAM … computers connect to shared cable which forms a ring.

iii) What is CSMA/CD and explain how it controls medium access and handles collisions. (6 marks)

Carrier Sense Multiple Access with Collision Detection. Protocol to manage access to a shared medium. Used by ethernet. Listens for the carrier on the cable. When in use station does not use cable. Waits a random amount of time before trying to send again. If not in use the station starts transmitting and continues to listen to the line. If a collision occurs, station stops transmitting and waits a random amount of time before retrying. The random delay is chosen between 0 and specified delay d. If another collisions occurs d is doubled – called binary exponential backoff.

iv) Describe how token ring controls medium access and collisions (3 marks)
Token circulates on ring, station that has token controls medium. Collisions avoided.

v) List three reasons why LAN extension technologies required? (1 marks)

vi) Briefly distinguish between repeaters, bridges and routers. (3 marks)
All used to extend max. distances of communication media. A repeater is usually an electronic device that allows two cables to be joined together. Repeaters operate at the physical layer and do not understand or interpret frames. Bridges are also electronic devices that operate at the Data Link layer. Bridges listen to traffic on each cable segment and forwards only those frames destines for the other segment. Routers are network level devices that are used to interconnect networks.

Question 5 (20 marks)
Answer all parts

i) Outline the different types of Web documents and their relative advantages/disadvantages. (8 marks)
Three basic types of Web documents

Static
Created and non-changing
+ easy to build
+ easy to test …ish
+ fast
+ longevity
•inflexible

Dynamic
Created dynamically by the Web server
+ flexible
+ can report current news e.g. stock prices
•slower than static
•increased cost
•testing more difficult

Not that both static and dynamic documents do not change once downloaded by a browser.

Active
Consists at least partly of a computer program
When running the program can interact with the user and change the display continuously
+ can update information continuously e.g. running an animated image
+ can access sources of information continuously and ergot update the display continuously e.g. stock prices
•increased costs
•lack of security

ii) Describe the Common Gateway Interface and the two methods of sending (6 marks)

user data to the server.

Building Dynamic Documents

A widely used technology is the **Common Gateway Interface** (**CGI)**

1. Specifies how a server interacts with an application
2. Does not specify what programming language to use
3. The URL specifies which program to run

Passing Parameters
Two methods of sending user data to the server:
GET and POST HTTP requests

- **GET appends the parameters to the URL**
- Parameters are accessed via the QUERY_STRING environment variable
- A '?' is placed at the end of the URL, parameters are placed after this

e.g. http://www.itcarlow.ie/cgi-bin/prog?hello

- POST sends the data in the optional data field of the HTTP request
- Passed to CGI program as standard input
    - like command line arguments

In both cases CGI program must decode the data

Simple CGI Example

```
#!/bin/sh
echo Content_type: text/plain
echo
echo Hello
echo This document was created on 'date'
```

CGI program should return a valid HTTP header through standard output

iii) Outline the main features of Active Server Pages. (3 marks)

Active Server Pages

- a HTML page that includes one or more scripts (small embedded programs)
- processed on a Microsoft Web server before the page is sent to the user.
- similar to the common gateway interface (CGI)
- Typically, interrogates a database and customizes the page before sending it to the requestor.

iv) What are sockets? (3 marks)

Sockets are a BSD operating system abstraction to allow users to write programs that utilize the underlying communication protocols. Unrelated processes on different nodes can communicate across the network by writing to and reading from sockets.
Sockets are bi-directional. Sockets sit on top of the transport layer, which provides an end-to-end connection across multiple networks.

Question 6 (20 marks)

Answer <u>FOUR</u> parts only. Each carries 5 marks:

i) Describe the main features of Asymmetric Digital Subscriber Line (ADSL)

- reserves more bandwidth going downstream (to the user - 255 channels for downstream transmission & 31 for upstream)
- most attractive to Internet surfers and users of remote LANs, because they typically download much more data than they send.

ii) Write short notes on checksums?

- Error detection mechanism
- Sum of data in message treated as array of integers
- Can be 8-, 16- or 32-bit integers
- Typically use 1s-complement arithmetic
- Example - 16-bit checksum with 1s complement arithmetic

iii) Describe how name resolution is handled by DNS.

- Resolver software typically available as library procedures
- Calling program is *client*
- Constructs DNS protocol message - a *DNS request*
- Sends message to local DNS server
- DNS *server* resolves name
- Constructs DNS protocol message - a *DNS reply*
- Sends message to client program and waits for next request
- Each DNS server is the *authoritative server* for the names it manages
- If request contains name managed by receiving server, that server replies directly
- Otherwise, request must be forwarded to the appropriate authoritative server

iv) What is byte stuffing and why is it used?

- *Bit stuffing* and *byte stuffing* are two techniques for inserting extra data to encode reserved bytes
- Byte stuffing translates each reserved byte into two unreserved bytes
- For example, can use esc as prefix, followed by x for soh, y for eot and z for esc:

Character In Data	Characters Sent
soh	esc x
eot	esc y
esc	esc z

v) Briefly describe the following transmission media: radio, microwave & infrared

- Radio
  - Data transmitted using radio waves
  - Energy travels through the air rather than copper or glass
  - Conceptually similar to radio, TV, cellular phones
  - Can travel through walls and through an entire building
  - Can be long distance or short distance
- Microwave
  - High frequency radio waves
  - Unidirectional, for point-to-point communication
  - Antennas mounted on towers relay transmitted data
  - Infrared
- Infrared light transmits data through the air
  - Similar to technology used in TV remote control
  - Can propagate throughout a room (bouncing off surfaces), but will not penetrate walls

Question 7 (20 marks)
Answer all parts

i) Describe the main features of TCP (5 marks)

- *Connection oriented*: Application requests connection to destination and then uses connection to deliver data to transfer data
- *Point-to-point*: A TCP connection has two endpoints
- *Reliability*: TCP guarantees data will be delivered without loss, duplication or transmission errors
- *Full duplex*: The endpoints of a TCP connection can exchange data in both directions simultaneously
- Stream interface: Application delivers data to TCP as a continuous stream, with no record boundaries; TCP makes no guarantees that data will be received in same blocks as transmitted
- Reliable connection startup: Three-way handshake guarantees reliable, synchronized startup between endpoints
- Graceful connection shutdown: TCP guarantees delivery of all data after endpoint shutdown by application

ii) Describe how TCP recovers from a lost packet (3 marks)

- TCP uses positive acknowledgment with retransmission to achieve reliable data delivery
- Recipient sends acknowledgment control messages (ACK) to sender to verify successful receipt of data
- Sender sets timer when data transmitted; if timer expires before acknowledgment arrives, sender retransmits (with new timer)

iii) Outline how TCP correctly orders incoming data (3 marks)

- Application delivers arbitrarily large chunks of data to TCP as a``stream"
- TCP breaks this data into segments, each of which fits into an IP datagram
- Original stream is numbered by bytes
- Segment contains sequence number of data bytes

iv) Describe how TCP manages flow control. (3 marks)

- TCP uses sliding window for flow control
- Receiver specifies window
- Called *window advertisement*
- Specifies which *bytes* in the data stream can be sent
- Carried in segment along with ACK
- Sender can transmit any bytes, in any size segment, between last acknowledged byte and within window size

v) Outline the process of connection establishment and termination as employed by TCP. (3 marks)

- TCP uses *three-way handshake* for reliable connection establishment and termination
- Host 1 sends segment with SYN bit set and random sequence number
- Host 2 responds with segment with SYN bit set, acknowledgment to Host 1 and random sequence number
- Host 1 responds with acknowledgment
- TCP will retransmit lost segments
- Random sequence numbers ensure synchronization between endpoints

vi) Outline the main features of UDP (3 marks)

- UDP delivers independent messages, called *datagrams* between applications or processes on host computers
- ``Best effort'' delivery - datagrams may be lost, delivered out of order, etc.
- Checksum (optionally) guarantees integrity of data
- For generality, endpoints of UDP are called *protocol ports* or *ports*
- Each UDP data transmission identifies the internet address and port number of the destination and the source of the message
- *Destination port* and *source port* may be different