BCS THE CHARTERED INSTITUTE FOR IT

BCS HIGHER EDUCATION QUALIFICATIONS
BCS Level 5 Diploma in IT

COMPUTER NETWORKS

APRIL 2015
EXAMINERS' REPORT

General Comments

Candidates are advised to read examiners' reports to prepare for their examination in this module.

Section A

Question A1

A1.This question is about fibre optic transmission systems.

a) Explain how data is transmitted along a fibre optic cable.
(6 marks)

b) Identify three physical characteristics of fibre optic cables that make them more suitable for high speed digital data transmission than copper cables.
(6 marks)

c) Describe what is meant by *wave division multiplexing* (WDM) and explain how it is used to deliver high rate data transmission over a fibre optic cable.
(6 marks)

d) A fibre optic transmission system uses wave division multiplexing with 16 different wavelengths of light. Each of these wavelengths is able to operate at 2.5Gbps. What is the maximum data carrying capacity of this transmission system? If you require 4Mbps to stream one high definition video, determine how many such videos could be transmitted at the same time using this fibre optic transmission system.
(7 marks)

Answer pointers

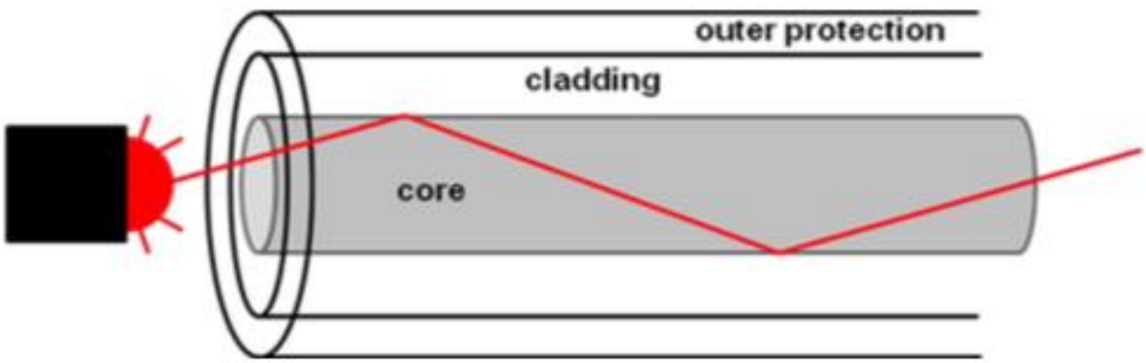
a)
Data is transmitted along a fibre optic cable as light using either a laser or LED.

The fibre core is made of a very thin strand of high purity glass.

The fibre core is surrounded by a cladding.

Light entering the core is reflected internally by the cladding and passes along the core with very little loss.

The outer layer simply provides protection for the core and plays no part in the transmission of signals.



(Marking scheme: 1 mark for use of light; 1 mark for LED or laser; 1 mark for fibre core being glass; 1 mark for cladding; 2 marks for internal reflection)

b)

Advantages over copper:

The fibre exhibits less loss (attenuation) than copper over the same length.

Fibre has less dispersion (distortion) than copper which allows for higher data rates to be achieved.

Fibre is less prone to external electromagnetic interference than copper and also does not itself generate such interference.

(Marking scheme: 2 marks for lower losses; 2 marks for higher data rates; 2 marks for being less prone to interference) c)

A fibre that uses only one wavelength of light is in effect a single channel.

Wavelength division multiplexing (WDM) is a technique used in fibre optics in which different wavelengths of light are transmitted along the same fibre.

Each wavelength carries its own data stream.

In this way multiple data streams are ‘multiplexed’ over the same fibre at the same time with each stream carrying its own separate data.

Therefore, the fibre comprises a series of transmission channels.

(Marking scheme: 2 marks for noting that different wavelengths of light (colours) are transmitted over the same fibre, 2 marks for noting that each wavelength carries its own independent data stream, 2 marks for noting that the different wavelengths are in effect multiplexed data channels leading to an increase in overall capacity is increased compared to a single wavelength fibre)

d)

Fibre system uses 16 wavelengths of light. Each wavelength operates at 2.5Gbps, therefore the total capacity of the fibre is 16 x 2.5 = 40Gbps.

(Marking scheme: 2 marks for 40 Gbps)

40 Gbps = 40 x 1024 x 1024 x 1024 bps (also accept: 40 x 1000 x1000 x 1000)

4 Mbps = 4 x1024 x 1024 bps

Therefore, total number of high definition videos

= (40 x 1024 x 1024 x 1024) / (4 x 1024 x 1024)
= 10, 240

(accept 10,000 when 1000 is used instead of 1024)

(Marking scheme: 2 marks for 40Gbps; 2 marks for converting Gbps to bps; 1 mark for knowing that you need to divide fibre capacity by the video bandwidth; 2 marks for final answer)

Examiner’s guidance notes

This question was attempted by about 89% of the candidates of whom just over half of them (54%) achieved a pass mark. The average mark was only 10 out of 25. There is evidence that the majority of the candidates were familiar with fibre optic transmission systems and managed well in parts a, and b. However, parts c and d attracted low marks, indicating that the topic of wave division multiplexing was not well understood.

Question A2

A2.This question is about the ISO Reference Model.

a) The ISO Reference Model defines seven protocol layers, each of which is responsible for a specific range of functions. By considering this model, explain the main functions performed by a protocol operating at:

i.The Physical layer
(3 marks)

ii.The Transport layer
(3 marks)

b) What is meant by the term peer to peer protocol?
(3 marks)

c) Give one example of a device on a network that is required to operate all seven layers of the OSI Reference Model.
(2 marks)

d) Figure 1 shows part of a network in which two personal computers A and B, are each connected to a switch (LAN switch 1 and 2) which are themselves interconnected by a router. Consider the transmission of data from personal computer A to B and produce a protocol layer diagram that clearly shows how data passes through all of the layers of the ISO Reference model that are used within the PCs, switches and router.
(14 marks)

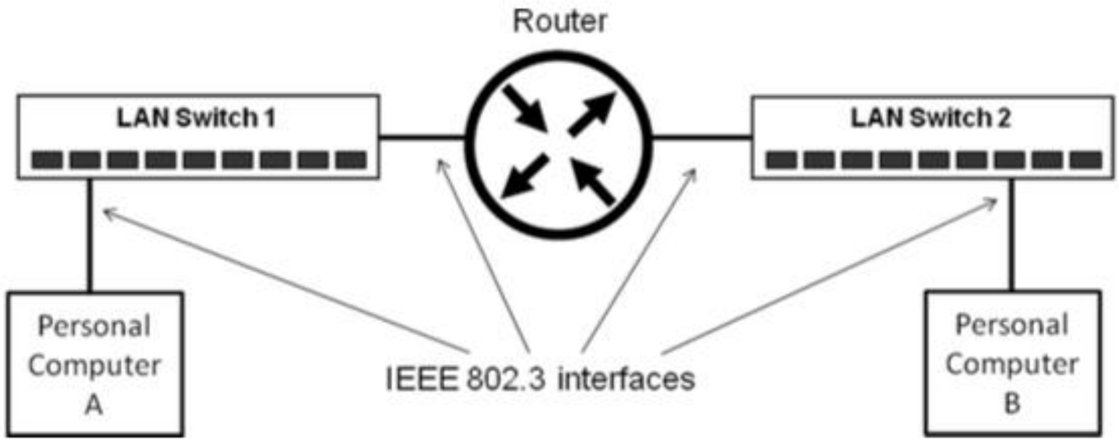


Figure 1

Answer pointers

a)

Physical layer

- Defines the electrical interface to a transmission medium
- The physical properties of the transmission medium
- The process by which digital data is represented on the transmission medium
- (coding)

(Marking scheme: 1 mark per point identified)

Transport layer

- Manages the end to end communications
- Responsible for multiplexing higher layer services
- Offers either a reliable (connection orientated) or unreliable (connectionless) service

(Marking scheme: 1 mark per point identified)

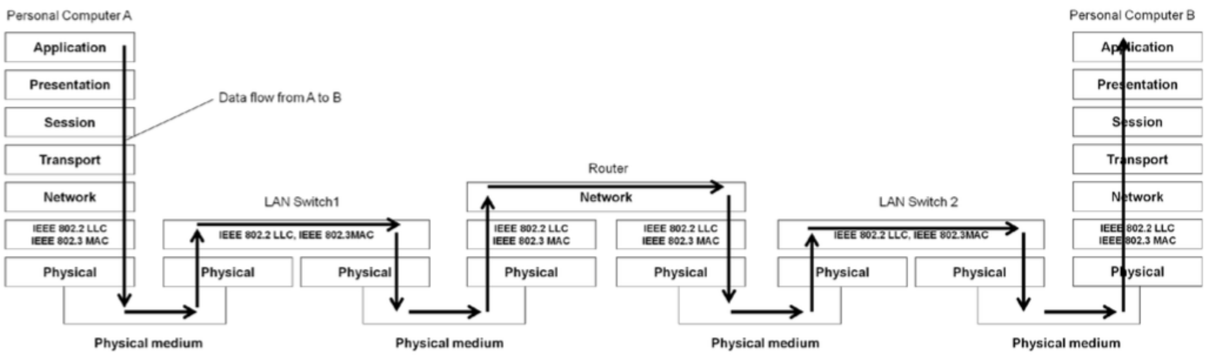
b)

In a layered protocol architecture data flows vertically through each of the layers of the model whereas protocols appear to operate horizontally. A peer to peer protocol is defined as the communication that takes place between two layers at the same level in different end- stations. (Marking scheme: 1 mark for protocol operating horizontally and 2 marks for communication between two layers at the same level.)

c)

End-station = personal computer, laptop etc. or
Server
(Marking scheme: 2 marks for either answer)

d)



(Marking scheme: 2 marks for PC A showing all 7 layers; 2 marks for switch 1 showing layer 2 spanning both physical ports; 4 marks for the router showing layer 3 spanning both ports with each port having its own layers 1 and 2; 2 marks for LAN switch 2; and 2 marks for PC B. 2 marks for showing the data flow from PCA to PCB.)

Examiner's guidance notes

This question was attempted by the largest proportion of candidates (95%) that attempted Section A. However, only about half of them (54%) achieved a pass mark, with the average mark being 9 out of 25. There is evidence that the candidates were well prepared on the OSI reference model and answered correctly part a. However, responses to part b varied as some candidates did not demonstrate knowledge of how to define peer to peer network. In part c, the majority of the candidates provided a correct example of a device that uses all seven OSI layers. Many of the candidates lost marks in part d for not correctly identifying the layers of a switch or router or indicating the data flow.

Question A3

A3.This question is about global network services and specifically a comparison between the Internet and Multi-protocol label switching (MPLS).

a) A global organisation has offices located in different countries around the world and wishes to connect these together with a network that can transfer data and telephone calls between each office. Explain how the Internet could be used to provide this network.
(4 Marks)

b) What limitations in terms of the Quality of Service it offers does the Internet have in respect of providing the network described in part A3a)?
(6 Marks)

c) How does the Quality of Service offered by Multi-protocol label switching (MPLS) differ from that offered by the Internet?
(6 Marks)

d) How could the global organisation described in part A3a) use Multi-protocol label switching (MPLS) to create its network and explain how MPLS would be able to provide a different Quality of Service for the transfer of data and telephone calls.
(9 Marks)

Answer pointers

a)

Each office would need to have a local connection to an Internet Service Provider (ISP) who in turn would provide access to the global internet.

Each office would then become part of the Internet and data could be transferred between them with a knowledge of the IP addresses that have been allocated to each office site.

(Marking scheme: 2 for each of the above points) b)

Internet QoS:

- The Internet is a best effort service which means that there is no guarantee that data will be delivered and if it is delivered, there is no way of predicting how long it will take.
- No differentiation – all traffic types handled equally which means that you cannot differentiate time critical application, such as the telephone traffic from non time critical ones, such as basic data transfer.
- The volume of traffic on the Internet cannot be predicted which means that the bandwidth being delivered between any two locations for a service cannot be predicted either.

(Marking scheme: 2 marks for each of the above points)

c)

MPLS network can establish single or multiple virtual circuits between offices.

Each traffic type can be allocated to its own virtual circuit which in turn can be offered a different class of service. Hence, the telephone calls can be differentiated from the data and given a different class of service.

MPLS is therefore able to offer a guaranteed QoS for all traffic passing over the network between the organisation's offices.

(Marking scheme: 2 for each of the above points)

d)

Each office would firstly need to be connected to the MPLS service through a single point of attachment.

Thereafter virtual circuits can be established through the MPLS network connecting each of the organisation's offices, with each virtual circuit having its own QoS.

As traffic enters the MPLS network, the ingress router classifies the traffic and allocates it to one of the virtual circuits and assigns a label to it.

All intermediate routers within the MPLS network process/route each packet based on the value of its label only. A given label is therefore linked to a specific QoS requirement and it is up to each router to ensure that packets are given the appropriate priority when being processed.

Telephone traffic has strict requirements in terms of the maximum transmission delay it can endure whereas data has no such restrictions. Therefore, it is important for the telephone traffic to be differentiated from the data by defining two classes of service. Labels will be assigned for each class of service and these will be allocated to each data packet as it enters the MPLS network and is classified.

On arrival at the final router in the route (egress router), the label is removed, and the packet transmitted to the destination.

(Marking scheme: 1 for each office attached through a single point of attachment, 1 for establishment of virtual circuits between offices, 2 for labels being assigned to virtual circuits, 2 for label switching within the MPLS network, 2 for telephone and data differentiation, 1 for removal of label at egress router.)

Examiner's guidance notes

This question was attempted by slightly over two thirds of the candidates (70%), of whom only a third (33%) achieved a pass mark. The average mark was a poor 6 out of 25. The evidence shows that many candidates confused MPLS with ADSL and provided the wrong definition. This was a poorly answered question indicating that the candidates did not have a clear understanding of MPLS and how it is used.

Section B

Question B4.

This question is about the main differences between IPv4 and IPv6.

a) IPv6 introduced the concepts of global unicast and link-local addresses. Provide a brief description of the differences between those addresses.

(6 marks)

b) Explain the reason why IPv6 addresses are represented in hexadecimal while IPv4 in binary.

(4 marks)

c) Write the shortest compressed format of the following IPv6 addresses:

- 2001:0DB8:0000:1470:0000:0000:0000:0200 (4 marks)
- F380:0000:0000:0000:0123:4567:89AB:CDEF (3 marks)

d) The dynamic assignation of Global Unicast IPv6 addresses can be done in two different ways: 1) Stateless Address Autoconfiguration (SLAAC) and, 2) Dynamic Host Configuration Protocol v6 (DHCPv6). Describe the differences between the two methods.

(8 marks)

Answer pointers:

a. Global unicast and link local addresses are a type of IPv6 unicast address. The keyword to understand them is in the name. A **global unicast** IPv6 address is globally unique, is an Internet routable addresses and can be configured statically or assigned dynamically. A **link-local** address is used to communicate with other devices on the same local link, it is confined to a single link and it is not routable beyond the link and it is automatically configured on the interface.

(Marking scheme: 3 marks for the three characteristics of a global unicast address; 3 marks for the three characteristic of a link-local address)

b. The key on this question is in the size of each type of address. IPv4 addresses have a length of 32 bits while IPv6 have a length of 128 bits. To make it easier for humans to manipulate these addresses the binary represented was proposed however, because of the length of IPv6 addresses, it was preferred to use hexadecimal as in can accommodate more values in one code.

The answer to this question is not related to the actual numbering system (binary or hexadecimal) but to the size of the IP addresses.

(Marking scheme: 2 marks for indicating the length of each address and 2 marks for the correct explanation)

c. A double colon (::) can replace any single, contiguous string of one or more 16-bit segments (hextets) consisting of all 0s, and can only be used once per IPv6 address. Any leading 0s (zeros) in any 16-bit section or hextet can be omitted. Therefore, the correct answers are:

i. 2001:DB8:0:1470::200
ii. FE80::123:4567:89AB:CDEF

(Marking scheme: 1 mark for each correct compression in the first address; 1 mark for each compression in the second address)

d. Stateless Address Autoconfiguraton (SLAAC) is a method that allows a device to obtain its prefix, prefix length and default gateway from an IPv6 router, no DHCPv6 server needed and it relies on ICMPv6 Router Advertisement (RA) messages.

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) works as in IPv4. It automatically receives addressing information, including a global unicast address, prefix length, default gateway address and the addresses of DNS servers using the services of a DHCPv6 server.

Device may receive all or some of its IPv6 addressing information from a DHCPv6 server depending upon whether option 2 (SLAAC and DHCPv6) or option 3 (DHCPv6 only) is specified in the ICMPv6 RA message. Host may choose to ignore whatever is in the router's RA message and obtain its IPv6 address and other information directly from a DHCPv6 server.
(Marking scheme: 4 marks for the SLAAC explanation; 4 marks for the DHCPv6 explanation)

Examiner's Guidance Notes:

Question 4 was the second most popular question of section B of the paper. It was attempted by 53% of the candidates but only 11% got a passing mark. There is evidence that most the candidates are not aware of IPv6 addressing scheme details. The purpose of the question was to evaluate candidates' knowledge on how IPv6 handles addressing and how it improves IPv4.

Question B5

This question concerns local area networks (LAN) technology and IEEE802.3 standards.

a) The data link layer in the IEEE standard is divided into two sublayers: LLC and MAC. Indicate the functions performed by each sublayer.

(5 marks)

b) Describe briefly the access method used by Ethernet including the way it handles collisions.

(6 marks)

c) Explain the reason why CSMA/CD requires a restriction on frame size for it to work and indicate the minimum value it should have.

(4 marks)

d) Use the following image to indicate the format of the IEEE 802.3 frame.

(7 marks)

2 bytes	**1 byte**	**6 bytes**	**6 bytes**	**2 bytes**		**4 bytes**

e) Explain the purpose of the length/type, Data and CRC fields of the IEEE 802.3 frame.

(3 marks)

Answer Pointers:

a. Logical Link Control: handles framing, flow control, and error control. Media Access Control: defines the access method and the framing format specific to the corresponding LAN protocol.

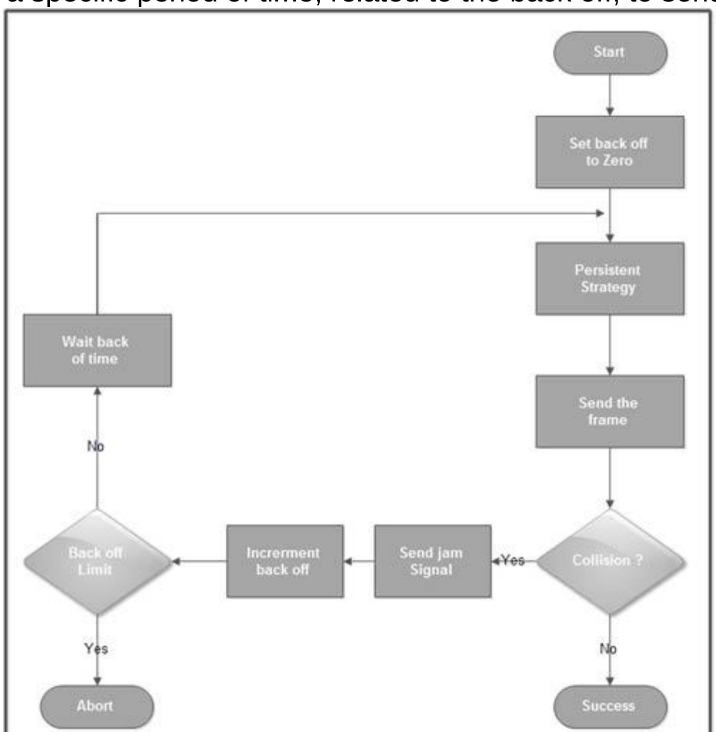
(Marking scheme: 1 mark per correct function in each sublayer)

b. There are three key elements for this question:

i. Back off mechanism. When the channel is being used, the device wanting to send must wait for a specific period of time.

ii. Persistent strategy. Devices wanting to send will continuously listen for the channel until it is free.

iii. Collision detection mechanism. If a collision occurs, the first device to detect it must send a jam signal, so the rest of the devices are aware of the collision and wait for a specific period of time, related to the back off, to send.



CSMA/CD Procedure

(Marking scheme: 2 marks for the back off mechanism, 2 marks for the persistent strategy, 2 marks for the collision detection mechanism)

c. For CSMA/CD to work, we need a restriction on the frame size. Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission.

This is so because the station, once the entire frame is sent, does not keep a copy of the frame and does not monitor the line for collision detection. Therefore, the frame transmission time must be at least two times the maximum propagation time Tp. To understand the reason, let us think about the worst-case scenario. If the two stations involved in a collision are the maximum distance apart, the signal from the first takes time Tp to reach the second, and the effect of the collision takes another time Tp to reach the first. So, the requirement is that the first station must still be transmitting after 2Tp. In Ethernet this value is 512 bits or 64 bytes.

(Marking scheme: 2 marks for the reasoning and 2 marks for the value)

d. A frame is the PDU of layer 2 of the OSI Model.

Preamble	SFD	Destination Address	Source Address	Length Or type	Data And Padding	CRC
2 bytes	**1 byte**	**6 bytes**	**6 bytes**	**2 bytes**		**4 bytes**

(Marking scheme: 1 mark per correct field)

e. Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field. Both uses are common today.

Data. This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.

CRC. The last field contains error detection information, in this case a CRC-32.

(Marking scheme: 1 mark per correct field; 1 mark per correct explanation)

Examiner's Guidance Notes:

Question 5 was the most popular question of section B but only by a small percentage. 54% of the candidates attempted this question and almost 30% got a passing mark. This question evaluates understanding of layer 2 implementation in the IEEE 802.3 standard.

A common error was for candidates to confuse the MAC sublayer with the MAC address, although physical addressing is part of layer 2 functionality, it is not covered in the MAC sublayer. Candidates also tried to explain the CSMA/CD mechanism by using a diagram, but they ended up drawing computers connected to a network. The section that most candidates got correct was the one related to the frame format, however there is evidence that many of them failed to demonstrate the correct order of the fields, but the majority remembered their name and purpose.

Question B6

This question is about error detection and correction.

a) Explain the concept of Hamming distance and how it is calculated.

(4 marks)

b) Explain the relationship between the Hamming distance and errors occurring during transmission and calculate the Hamming distance between 01011 and 10101.

(6 marks)

c) Indicate and explain what would be the minimum Hamming distance for error detection and the minimum for error detection.

(10 marks)

d) A code scheme has a Hamming distance d_{min} = 4. What is the error detection and correction capability of this scheme? Explain why part of the capability of the system is wasted.

(5 marks)

Answer pointers:

a. The Hamming distance between two words (of the same size) is the number of differences between the corresponding bits. We show the Hamming distance between two words x and y as d (x, y).

The Hamming distance can easily be found if we apply the XOR operation on the two words and count the number of 1s in the result. Note that the Hamming distance is a value greater than zero.

(Marking scheme: 2 marks for the explanation and 2 marks for how it is calculated)

b. When a codeword is corrupted during transmission, the Hamming distance between the sent and received codewords is the number of bits affected by the error. In other words, the Hamming distance between the received codeword and the sent codeword is the number of bits that are corrupted during transmission.

For the d(01011, 10101), we need to apply the XOR operation on the two words:

01011
<u>10101</u>
11110

The count of the number of 1s is 4, therefore d(01011, 10101) is 4

(Marking scheme: 4 marks for the explanation and 2 marks for the calculation)

c. Minimum distance for error detection: If we want to be able to detect up to s errors. If s errors occur during transmission, the Hamming distance between the sent codeword and received codeword is s. If our code is to detect up to s errors, the minimum distance between the valid codes must be s + 1, so that the received codeword does not match a valid codeword. In other words, if the minimum distance between all valid codewords is s + 1, the received codeword cannot be erroneously mistaken for another codeword.

Minimum distance for error correction: If s errors occur during transmission, the Hamming distance between the sent codeword and received codeword is s. If our code is to detect up to s errors, the minimum distance between the valid codes must be s + 1, so that the received codeword does not match a valid codeword. In other words, if the minimum distance between all valid codewords is s + 1, the received codeword cannot be erroneously mistaken for another codeword. The distances are not enough (s + 1) for the receiver to accept it as valid. The error will be detected.

(Marking scheme: 5 marks for explaining the minimum distance for error detection and 3 marks for the minimum distance for error detection)

d. This code guarantees the detection of up to three errors (s == 3), but it can correct up to one error. In other words, if this code is used for error correction, part of its capability is wasted. Error correction codes need to have an odd minimum distance (3, 5, 7, ...)

(Marking scheme: 3 marks for the capability of the scheme and 2 marks for the explanation of the waste of the system)

Examiner's Guidance Notes:

Question 6 of section B was the least popular amongst the candidates. Only 26% of the candidates attempted the question with only 2% obtaining a passing mark. This question can be considered the most complicated of them all mainly because it uses binary representation and the binary XOR operation. There is evidence that some candidates demonstrated knowledge of the subject and tried to answer by explaining other type of error detection and correction methods but failed to identify how Hamming distance works.