9.3 The internet part 2 Mark Scheme

Q1.

World-Wide Web:

A1. a system of interlinked hypertext documents;
A2. accessed via the Internet;
A3. using HTTP protocol (to retrieve webpages);
A4. Web pages not restricted to intranet;

Internet:

B1. global network;
B2. A network of interconnected computer networks / computers;
B3. using a globally unique address space;
B4. Packet-switched network;
B5. using end-to-end communication protocol // Internet Protocol // TCP / IP;
B6. public network;

Intranet:

C1. a private (computer) network;
C2. available to a closed community // only within an organisation;
C3. that uses Internet Protocols;
C4. to share part of an organisation's information (with its members);

To achieve a mark in this band, a candidate must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QLx).

SUB Candidate has provided a clear explanation of at least 5 differences listed above between the three terms.
QL1 Text is legible.
QL2 There are few, if any, errors of spelling, punctuation and grammar. Meaning is clear.
QL3 The candidate has selected and used a form and style of writing appropriate to the purpose and has expressed ideas clearly and fluently.
QL4 Sentences and paragraphs follow on from one another clearly and coherently.
QL5 Appropriate, specialist vocabulary has been used.

5–6

To achieve a mark in this band, a candidate must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QLx).

SUB Candidate has provided a limited explanation of at least 3 differences between at least two of the terms.
QL1 Text is legible.
QL2 There may be occasional errors of spelling, punctuation and grammar. Meaning is clear.
QL3 The candidate has, in the main, used a form and style of writing appropriate to the purpose, with occasional lapses. The candidate has expressed ideas clearly and reasonably fluently.
QL4 The candidate has used well-linked sentences and paragraphs.
QL5 Appropriate, specialist vocabulary has been used.

3–4

To achieve a mark in this band, a candidate must meet the subject criterion (SUB). The quality of language should be typified by the QLx statements.

SUB Candidate has provided a weak explanation which does not demonstrate a

clear understanding of the differences between the three terms, or only one or two differences given.

QL1 Most of the text is legible.

QL2 There may be some errors of spelling, punctuation and grammar but it should still be possible to understand most of the response.

QL3 The candidate has used a form and style of writing which has many deficiencies. Ideas are not always clearly expressed.

QL4 Sentences and paragraphs may not always be well-connected or bullet points may have been used.

QL5 Specialist vocabulary has been used inappropriately or not at all.

1–2

Candidate has not made reference to any of the points listed above.

0

Note: even if English is perfect, candidates can only get marks for the points made at the top of the mark scheme for this question.

If a candidate meets the subject criterion in a band but does not meet the quality of language criteria then drop mark by one band, providing that at least 3 of the quality of language criteria are met in the lower band. If 3 criteria are not met then drop by two bands.
Must mark quality of language and contents holistically, not separately.

[6]

Q2.

(a) (i) IP address / Internet Protocol Address;

1

(ii) Uniform Resource Locator;
A Universal Resource Locator

1

(b)
- Forwards / backwards / Navigation – move to a previously viewed page;
- Favourites/Bookmarks – setting up/organising/stores regularly visited sites;
- Options/Tools/Settings – setting up of the Home page / enable/disable features e.g. run JavaScript;
- Home – move to the Home page;
- Refresh – refresh the current page;
- Stop – stop loading the current page / download;
- History – show a list of the last (say) 20 pages displayed;
- Security – change settings / e.g. enable/disable graphics/pop-ups/other content/plug-ins;
- View HTML – source (code);
- Address bar – allows the entering of a URL/IP/web address;
- Search bar – search list for specific web site;
- RSS feeds – receiving content news/updates;
- Application launcher icon e.g. to run email client application;

R HTML editor

Feature followed by NO description scores 0
Good description with feature implied scores 1

Max 2

(c) (i) footyhosting.co.uk

1

(ii) (Each hosted club has) a (sub) folder/directory containing the files for their site;

1

(d) 128 kbps // 2Mbps // 128 kbps AND 2Mbps;
R answers where in addition any other answer is circled

1

(e) (i) (magnetic/server) hard disk/ hard drive;
R removable hard disk
A 'disk' spelt as 'disc'

1

(ii) 8000 GB;

1

[9]

Q3.

(a) Hidden camera to record you entering your PIN;
Watch as the PIN is keyed in;
False keypads / key logger; **R** key logger on PC Phishing;
Hacking into servers / records where card data is stored;
Searching through dustbins to find documents/ interception;

R skimming, spyware, cloning devices

2

(b) By the padlock in the bottom right hand corner of the screen
/ the browser's indication of a secure site;
/By the protocol HTTPS;
/It has an authentic certificate;

1

(c) Encryption;

A use SSL

1

[4]

Q4.

(a) **Symmetric key encryption:** the same key/process/algorithm is used for encrypting and decrypting;
A sending/receiving instead of encrypting/decrypting public key encryption:
Public Key enscryption: a public key and a private key // a pair of keys are used in combination; one to encrypt, the other to decrypt;

3

(b) (i) **When:** the symmetric key is sent (from B to A)
// when establishing the initial connection;
How: B must encrypt the symmetric key; with A's public key;
so A can decrypt (the symmetric key) with A's private key;
A A must encrypt the symmetric key; with B's public key;
so B can decrypt (the symmetric key) with B's private key;

Max 3

(ii) Anyone could intercept the message with the symmetric key (and then decrypt the personal data);
distributing the symmetric key securely is not possible (unless it is encrypted);
R unspecific answers such as 'easily hacked'

1

[7]

Q5.

(a) If computer wants to send message/packet to an IP address not on same subnet/network // if computer wants to access the internet;
T.O. if implied that all messages are sent to the gateway sends the message/packet to the gateway; which has the IP address subnet.1;

Answer must imply communication not just connection or access

2

(b) Domain name is intercepted by a domain name server;
Domain name server looks up domain name in its database/table/list;
Finds matching IP address;
If it can't find domain name, contacts another Domain Name Server;

The answer must imply the idea of a look up not somehow a conversion which might be a calculation

Max 2

[4]

Q6.

Message/data broken down into packets;
source/destination (address) is added to each packet;
message ID added to each packet;
packet sequence number added to each packet; A numbered packet;
each packet may well travel along different paths to get to the final destination
// packets routed independently;
recipient puts packets into correct sequence
// packets reassembled into message at destination;
checking for errors (and resend packets)
// request for corrupted packets to be resent;
// a virtual circuit is established // packets are sent over a virtual circuit;
(allow for non-IP packet switching answers eg. X25 or ATM)

Max 3

[3]

Q7.

(a) (i) Computers/devices/nodes/PCs connected/linked/communicate together;
R machine
A using a LAN protocol e.g. Ethernet

Over a small geographical area / e.g. a room/a building /a site ;

2

(ii) Bus ;

R line

1

(iii) Serial ;

1

(iv) Ring // star ;

1

(v) Printer; (bar code) scanner; multifunction machine ; modem ; message boards ; server
Providing audio/video or any additional server; console dedicated to audio/video ;
Projector ; FAX machine ; external hard drive ; card reader ;
A bridge / hub, / switch / router / gateway / firewall ;

Max 2

(b) (i) Bargainbooks-r-us.co.uk ;
R answer with anything added to this

1

(ii) The file (name); the page requested; home page;

Max 1

(iii) The web server cannot find the page requested //
(examples) the page has been deleted / moved to different folder / does not exist ;
the page is in the process of being updated / page is currently off-line;
R anything which implies there is no connection
R timed out

2

(c) (i) Computers (and networks) connected/linked/communicating ;
A using a WAN protocol e.g. TCP/IP
Over a large/wide geographical area / e.g. city/county/country/ globally / e.g. The Internet ;
R WWW

1

(ii) E-mail communication with the outside world (A or B) ;
Email/easier communication between libraries // the library and a borrower (A or B) ;
Enquiries about books available at other libraries (A or B) ;
Electronic transfer of documents/information between libraries (A only) ;
Backup of data/network administration for all libraries is more manageable/done centrally (A only) ;
A Accept benefits which imply access to the World Wide Web / Internet (A or B) ;

Max 2

[14]

Q8.

(a) (i) An internal web site/set of web pages // web site local to an organisation ;
(Web) pages which can only be viewed with authority/provided with access from the organisation ;
A provides internet facilities within the organisation
A a LAN which uses internet protocol ;

R Local internet
R LAN description (alone)

Max 1

(ii) Access to / links to resources for learning / access to subject sites ;
Anything related to the menu bar ;
Access to resources about College facilities ;
Info about / news items / read the student bulletin / exams certificates;
Links to UCAS / writing a personal statement / Student council / use the search engines / access to external web sites

Max 2

(b) (i) Hypertext transfer protocol // protocol;

1

(ii) The pages to be accessed are on the world wide web / (the pages accessed are from) a web site ;
R world wide web (only)

1

(iii) The domain name / XYZCollege.ac.uk is the College's domain name;
The domain name is registered in the United Kingdom ;
R hosted
In' ….'
.ac is an academic/educational institution / .ac is the type of institution ;
A .ac.uk is the type of site / is the top level domain
The alternative to using/the user friendly version of the IP address // has an equivalent IP address ;
What is held on a Domain Name Server;

Max 2

[7]

Q9.

(a) If you send the key with the message, anyone can decrypt the message.

Key would need to be sent by means other than email, otherwise anyone could intercept the key and use it do decrypt the message;

1

(b) (i) Jill's public key;

1

(ii) Jill's private key;

1

(c) (i) The message data is hashed into a message digest;
The message digest is encrypted; with the sender's private key;

3

(ii) Jill's software decrypts the signature;
Using Jack's public key; contained in digital certificate sent with message;
To verify Jack's public key;
Decrypt digital certificate using Certificate Authority's (trusted third party's) public key;
Jill's software then hashes the document data into a message digest;
If recalculated message digest is the same as the original message digest (decrypted signature);

Then Jill knows that the signed data has not been changed;
I decryption of message

4

[10]

Q10.

(a) Allows for the sharing of peripherals/hardware; **R** 'Resources' programmers can access their work from any terminal; better communications / internal e-mail/instant messaging; easier/quicker/instant sharing of a program library/ sharing program code/ data files; central storage of documents e.g. program specifications; changes to important documents are held centrally / document management; setting up of an Intranet (for document management); easier for the backup of data;
R anything about program updates

Max 2

(b) (i) Easier/quicker installation/maintenance of the application software / easier backup (only if not in(a));
R Saves space on the PCs / 'Security' / cheaper (licensing)

1

(ii) If server goes down software (may) still be available;
Software will load/accessed faster from secondary store;
Software can be personalised for individual user;
Helps to avoid degradation in network performance;
R anything about the software runs faster

1

(c) (i) Protocol set of rules (about the way devices communicate);
A standards
R Instructions

1

(ii) Handshaking …
Sending signals between devices + implication of 2-way;
Confirmation of ready for sending / receiving data;
Acknowledge that a transfer is completed;

Max 2

(d) smk-solutions.co.uk;
R www.smk-solutions.co.uk

1

[8]

Q11.

(a) Browser / web browser / Internet browser;

1

(b)
- forwards/backwards a page;
- address bar for the display of the URL;
- setting up/organising 'Favorites' pages;
- setting up of the Home page;
- move to the Home page;
- refresh the current page;
- stop loading the current page/ download;
- history - show a list of the last (say) 20 pages displayed;

- security - change settings /e.g. enable/disable graphics/pop-ups/other content/plug-ins;
- browsing - change settings;
- view (HTML) source (code);

R HTML editor

Max 2

(c) StationeryIsUs.co.uk/default.htm // www.StationeryIsUs.co.uk/default.htm;
A StationeryIsUs.co.uk // www. StationeryIsUs.co.uk
I. http:// ignore case

1

(d) IP address (which matches with this URL); R. IP number

1

(e) uk / co.uk / com / gov / tv / biz / net / org / ed / mil / info or from any other country eg fr ,it
A co.uk / ac.uk / sch.uk

Any two for 1 mark

1

[6]

Q12.

(a) Converting/transforming from plain text into ciphertext/secret code;
A scrambled;
A transposition / conversion / coding
The sender processes the message prior to transmission so that if it is accidentally or deliberately intercepted while it is being transferred it will be incomprehensible to the intercepting party;
Data coded so that unauthorised users can't read or access the data;

Max 1

(b) (i) B's public key;

1

(ii) B's private key;

1

(c) (i) A hashing function is applied to the text of the message; the result/message digest is encrypted; using B's private key;
A the data generated is added to the end of the message;
A message/date stamp is used to produce digital signature;

Max 3

(ii) A uses Certificate Authority's public key; to verify B's public key;
Digital signature is decrypted;
Using B's public key;
The hashing function is applied to the text of the message;
The result of the hashing function is compared with the digital signature;
If they are the same the message is authentic;

Max 4

[10]

Q13.

(a) (i) World-wide collection of networks/computers using TCP/IP;

World wide collection of networks/ gateways/ servers/ computers
Using a common set of telecommunications protocols to link them together;
World-wide collection of networks/ computers using the same protocol;
World-wide collection of networks/computers using a standard protocol;

1

(ii) Collection of servers using Hypertext Transfer Protocol/HTTP//
Collection of data files/ documents using Hypertext Mark-up Language/ HTML/ XHTML/ XML;

1

(iii) Computers connected within a small geographical area/building/site;
A computers connected using local area network/LAN protocols;

1

(iv) Computers connected over a large geographical area;
A computers connected using wide area network/WAN protocols;

1

(v) Network providing Internet facilities within an organisation/ LAN using Internet protocol;

1

(b) (i) Any valid domain name, e.g. aqa.ac.uk;
R www.aqa.ac.uk

1

(ii) Any valid address in the range 0.0.0.0 to 255.255.255.255;

1

[7]

Q14.

(i) Hypertext transfer protocal//protocal (used) // set of rules (used);
R http format

1

(ii) www means it is a web site / web page / is on the web / on a web server;
R Internet
R world wide web on its own (n.e.)

1

(iii) (org means it is) an organisation/non-profit making;
A the type of organisation

1

(iv) The country of origin//based/registered in the UK;
A site in the UK
R country on its own (n.e.)

1

(v) The folder name//the subdirectory;
A the directory;

1

(vi) The file name//the page to be viewed;
A the document name

1

[6]

Q15.

(a) World-wide collection of networks/ computers using the same protocol;
World-wide collection of networks / computers using a standard protocol;
World-wide collection of networks / computers using TCP/IP;
World wide collection of networks / gateways / servers / computers using a common set of telecommunications protocols to link them together;

Max 1

1

(b) Name used to reference Internet connected computer / User friendly reference that maps to an IP address;
R Web site name / address
R example

1

(c) Network providing Internet facilities within an organisation / LAN using Internet protocol;

1

(d) Protocol used + address of resource (in two parts: the server and then the path to the resource on this server) / Uniform Resource Locator;
R example

1

(e) Numerical address / Stored in 4 bytes / Range 0.0.0.0 to 255.255.255.255/ Used to identify an individual computer / Internet Protocol address;
R example

1

[5]

Q16.

(a) bbc.co.uk; www.bbc.co.uk;

1

(b) (i) (hypertext transfer) protocol / protocol used / set of rules used;
R http format

(ii) www means it is a web site/web page/is on the web; **R** Internet
on a web server/the machine name;
world wide web on its own n.e.

(iii) (bbc is the)) organisation's/company's name/keyword/identifier/ site name/site owner;

(iv) (co means it is a) company; **A** corporation; the type of organisation;

(v) uk means the country of origin is the UK/based in UK/**A** site in the UK; where it is based/located;

(vi) History is the folder name/subdirectory
(which contains a file with default name of index.html);
OR **A** history is the page/filename of the web site/part of the site;

A (specific) topic;

6

(c) (i) Domain name has a single IP address;
Computer looks up domain name on a (domain) name server
Which tells the computer the IP address;
Domain name is user-friendly representation of IP number;
IP number/address is numerical representation of domain name;
Domain name maps onto IP address; one-to-one;

1

(ii) 0.0.0.0 / 0;
To 255.255.255.255 / 2^{32}-1 / 256^{4}-1; 4294967295;
Each group of digits is in the range 0-255;;

2

[10]

Q17.

(a) E-mail may pass through many computers/servers if it travels over a network, each computer can make a copy/can be accessed;
When a message arrives at its destination, it waits until the intended recipient picks it up. During this time the message is vulnerable to being read or copied by the computer's operator;
Electronic eavesdropping of telephone wires and local area networks is possible;
With e-mail alterations leave no trace(no physical damage) whereas with paper alterations leave a physical mark;

Max 1

(b) (i) E-mail encrypted using public key;
Recipient's private key used to decrypt e-mail;

2

(ii) E-mail encrypted by sender using private key;
Recipient decrypts e-mail using sender's public key;

2

[5]

Q18.

(a) (i) Share printer; share database; central backup possible;
Data consistency; electronic messaging/communication;
Share data/information/files/software; access files from any computer;
Easier to upgrade software;

Max 2

(ii) Network adapter/network card; **R** modem

1

(b) (i) More secure;
If a cable breaks only one node is out of action; **R** computer instead of cable performance does not degrade with increase in traffic;
Easier to find cable fault;

Max 1

(ii) Cheaper to set up; less cable needed;

Max 1

(c) (i) The name of an internet site/user friendly id of an internet site;
R address

1

(ii) (www.)companyname.co.uk *(any valid domain name)*

1

(iii) *Does not need www, could be ftp or wap also*

1

(d) A communication system providing similar services to the Internet;
Solely within a particular company or organisation/company wide;
An internal; internet;

Max 2

[9]

Q19.

(a) (i) www means it is a web site / web page/is on the web;
R internet

1

(ii) .aqa is the organisation's/company's name/keyword/identifier;

1

(iii) .org means it is a non-profit-making organisation / type of organisation/company;

1

(iv) .uk means the country of origin is the UK / based in UK;

1

(b) Computer looks up domain name on a (domain) name server which tells the computer the IP address;
Domain name is user-friendly representation of IP number;
IP number/address is numerical representation of domain name;
Domain name maps onto IP address;

Max 1

[5]

Q20.

Packet:
Data split into packets
Each packet finds its own route
From computer to computer / node to node
Could be by example such as internet

Any 2

[2]

Q21.

Store table of user-ids and student names
Record user – id of person who is on particular machine
Record web – sites visited by machine
Cross-referencing allows trace back to individual
Depending on the candidates school set up various combinations are possible but

the two points are (i) being able to record Internet activity and (ii) linking this to an individual

NOT simply "by audit trace/trail" since auditing system given in question

[2]

Q22.

Ill trained/ inexperienced users
Fire/Explosion
Burglary
Hardware Failure
Software Failure
Viruses
Hackers
Disgruntled Employees

Any 3
1 mark for each risk + 1 mark each suitable defence

[6]

Q23.

Hardware and (2) software conventions (rules) used to control the transmission of data (2)

[4]

Q24.

(a) Program designed to replicate itself (and spread on its own), preferably without anyone aware of its existence.
Damage files / hardware or amuse user

Any 2 × 1

2

(b) For each method given
2 marks for good description
1 mark for confused description
Methods can be drawn from any of the four groups.

Preparation/ prevention - Write protect all floppy disks make regular back ups restrict use of floppy disks Scan new software source disks with anti- virus software on a stand alone/ non- network computer networks restrict floppy drives.

Detection - Be aware of evidence for known viruses e.g. date virus
look for unexpected signs of virus activity: unexpected disk accesses: changes to program **files:** presence of unusual files in directories.

Containment - Disconnect an infected machine if necessary stop immediately a computer's activity on detection of any of the above scan any new software to be installed on the computer network for viruses restrict the use of floppy disks on networked computers.

Recovery - Replace infected files with clean back ups scan all files on computer with virus software" Tracing possible sources of infection" if qualified appropriately could appear in more than one category,

Any 4 × 2

8

(c) Could be a new virus not known to the virus detection software a virus which loads before the virus detection system is itself loaded may be able to hide its activity from the protection software by residing in the boot sector of a disk. Virus checker needs to be switched off before installing software

Any 2 × 1

2

[12]

Q25.

(a) Network connecting together geographically remote computers (separate sites/connected by phone lines/satellites/Internet)

1

(b) Rules (1) used to define the ways in which different (1) computer networks/computers may be connected to each other. (For rules do not accept standard)

2

(c) Need common standard (1) / because machines/networks different. (Needs idea of transmission) /to enable successful communication

1

[4]

Examiner reports

Q1.

Very few candidates found it difficult to organise their answer to this question and the quality of language used was generally high. Candidates often had no clear understanding of the difference between the World Wide Web, the Internet and an intranet; some even confusing the Internet with the World Wide Web. A significant number of candidates clearly had studied the relevant chapter in the text book very carefully, gaining full marks on quoting almost verbatim the definitions of the three terms.

Q2.

(a) Generally this question was consistently well answered.

(b) The marks were given were this time for a description of the feature (not just stating the name of the feature as in previous papers). The most popular answers were 'Page Navigation', 'Favourites', and 'History'. Some candidates did describe a feature which was not browser-specific such as 'Help' or 'Print', ignoring the rubric in the question stem.

(c) Any candidate who had practical experience with website construction would not have found a problem in identifying the use of folders/directories. Wrong answers, including vague answers, were 'by having a home page for each club', 'a home page with links to each club,' or, 'by having the club name at the end of the URL.'

(d) Most candidates achieved the mark, although seriously wrong answers included removable drives, DAT and even 'hard copy'!

Q3.

Most candidates gave creditable ways in which fraudsters could obtain a PIN without the owner's knowledge. Key logging on your computer was not accepted, as you never have to enter your full PIN when making an online purchase. Other methods such as hidden cameras, phishing or simply watching over your shoulder were all credited. A significant number of candidates seem to think the PIN could be found on their bank statement.

A purchaser can tell that a site is secure when making an online purchase by the symbol, typically a small closed padlock in the bottom right hand corner of your browser window. Alternatively, a protocol of https denotes a secure site. Typically, personal data is encrypted when being transmitted to or from a secure site.

Q4.

The topic of this question seemed to be understood very poorly. Many answers were seen where rote-learning was only partially successful and the part-remembered answers made little sense. Real understanding is required to be able to answer these questions successfully.

For part (a) symmetric encryption uses the same key for encryption and decryption, whereas public key encryption uses a public key – private key pair in combination, one to encrypt the other to decrypt.

In part (b), since few candidates understood the difference between symmetric and public-key encryption, the point of this question evaded many candidates. The symmetric key needs to be communicated securely to the other party. Therefore, it must be

encrypted with the Public key of the recipient. The recipient can then decrypt it with their own private key. Encrypting with the private key and decrypting with the public key is not appropriate here, as anyone intercepting the message could decrypt the encrypted symmetric key.

Q5.

(a) Few candidates could explain clearly how the default gateway address is used by a host computer. Some confused the default gateway address with a gateway connecting networks with different protocols. Some were under the impression that all messages were sent to the default gateway, whether intended for the same subnet or not.

(b) Most candidates could explain that a domain name server provided an IP address for a requested domain name. Fewer candidates could give a fuller explanation that the domain name server intercepts the domain name and looks up the domain name in its database to find the matching IP address. A small minority correctly stated that if the domain name server can't find the domain name in its database, that it will contact another domain name server.

Q6.

Packet-switching networks were very well understood by some candidates, but others gave very confused statements. Most candidates could explain that the data was broken down into fixed sized packets and that they might travel along different paths to their destination where the message would be reassembled. Fewer candidates could state clearly that each packet would also contain source and destination addresses as well as a message ID and a packet sequence number.

Q7.

In general candidates performed well on this question.

(a) (i) There were two key concepts required for the two marks. The idea that computers are connected and then proximity, usually explained by the candidate through example e.g. within the same building.

(ii) (iii) and (iv) Were all generally well answered.

(v) Most common answers were printer and scanner, although some more perceptive answers described a server which offered some service to the users of the network.

(b) (i) The old chestnuts were the inclusion of the www or the omission of the .co.uk to or from the domain name and, although one of these errors was allowed as an A (acceptable) answers on previous papers, it did not gain credit. Also spelling errors were penalised.

(ii) All that was required for the mark was an appreciation that this refers to the page. Many candidates described it as the folder where the file was to be found (again, probably thinking back to previous questions where the URL had included a folder).

(iii) Many candidates wrongly thought that this must be because the web site was unavailable and offered a variety of possible reasons. Any answers which implied there was no connection to this site did not score the mark.

(c) (i) The same thinking applied here as for (a) (i); the idea that there were multiple computers or networks connected, and for the second mark an explanation of 'wide area'.

(ii) The most common failing was for candidates was to describe a borrower and an administrator benefit which were in effect the same, and so scored only one of the two available marks. 'Administrator' was taken in its most general form, and answers which described a benefit to a network administrator were considered acceptable. The most common wrong answer was that "borrowers would be able to return books to other libraries" (when the rubric of the question stated that "There is no system for the exchange of books between libraries").

Q8.

(a) (i) A variety of possible answers were on the mark scheme but the better candidates were clear that an Intranet refers to the content which LAN users are able to access.

(ii) Answers were often vague but did still gain credit as they could be inferred from links or other web page content shown in the diagram.

(b) This question has now been asked on several previous papers but there are some candidates who are still giving answers which are insufficient. On what is potentially an easy question – and again, which is embedded in their student experience – answers were often weak. The key word in the stem of the question was 'explain' so answers such as "world wide web" are not a sufficient answer where the requirement is to explain. For the explanation of the .uk, candidates must appreciate there is a significantly different interpretation of their answer depending on their use of English; "based in" – "hosted in" – "registered in" all have very different meanings.

Q9.

(a) Very few candidates appreciated that the issue with encryption of e-mails using symmetric keys is how to get the key from the sender to the recipient. Some wrongly thought that the key would have to be made public, or that all e-mails would have to use the same key.

(b) Most candidates stated correctly that Jack would need to encrypt the message with Jill's public key and then Jill could decrypt it with her private key. Some candidates did not state whose public/private key was required to be used, and so did not gain the marks available.

(c) There seems to be a lot of uncertainty about what a digital signature is or how it might be produced. It is not a signature in the conventional sense. Candidates who gained full marks could explain that the message (before encryption) was hashed into a message digest, which was then encrypted using the sender's private key.

(d) The lack of understanding of digital signatures was further highlighted by the responses to this part of the question. Verifying Jack's digital signature means, to ensure that the message really was sent by Jack, Jack will need to have sent a digital certificate with the message, containing his public key. The digital certificate needs to be decrypted using the Certificate Authority's public key, ensuring that the digital certificate is genuine. Now the signature sent with the message can be decrypted using Jack's public key. The received (and decrypted) message is hashed and the result is compared to the decrypted signature. If both are the same the message has not been tampered with and is genuine.

Q10.

When any question asks for 'advantages or disadvantages" then candidates should not fall into the trap of the 'quicker/faster/easier' answer.

(a) In this part as well as part (b) the mark scheme had a wealth of acceptable answers and candidates generally scored well, often with answers which came from their own experiences of a school/college network. A common wrong answer was that "only one copy of the software need be purchased".

(c) (i) Most candidates scored the mark for a 'a set of rules" but the suspicion that their understanding went no further than that was confirmed by the answers seen for (ii).

(ii) Candidates who had the basic understanding of a two way exchange of signals or acknowledgments should have been able to score 2 with a general statement, followed by a description of a particular signal. Although not required in this question, candidates should also appreciate that particular lines/wires of the connecting cable will be used to transmit these signals.

(d) There are still some candidates who include the 'www' as part of the domain name. For the first time an answer which included the 'www' as part of the domain name scored zero.

Q11.

Most candidates scored well on this question.

(a) There were still some scripts where the candidates suggested a brand name such as Internet Explorer, and consequently scored zero.

(b) The question asked for 'features' and the majority of candidates were able to describe these. The common wrong answer was to just say what a browser does i.e. display web pages, and not describe specific features, which were generally well known. One-word answers however were very common.

(c) This part was well answered by many candidates.

(d) IP addresses appear to be well understood.

(e) Some candidates lost the mark with the inclusion of some domain name before the top-level identifier.

Q12.

This question was either very well done, by those candidates who had a clear understanding of the principles involved, or very poorly done by those who only had a vague notion of how this important aspect of security on the Internet works.

(a) Many candidates found it difficult to express clearly what encryption was. A creditworthy response was converting plain text into cyphertext.

(b) Many candidates failed to realise that both A and B had a private and a public key. The answer therefore needed to include whose public/private key should be used.

Sending a message that only B can understand must be encrypted using B's public key, so that only B's private key can decrypt the message.

(c) There seems to be much confusion as to what a digital signature is and the role of a digital certificate. Here is an explanation:

So that the digital signature will show up any tampering of the original message, the digital signature is based on the (date-stamped) message: a hashing algorithm is applied to the text of the message. This produces what is known as a message digest. So that this cannot be substituted when the message is tampered with, it is encrypted with the sender's private key and attached to the message.

The recipient can decrypt the signature with the sender's public key.

To check that the message has not been tampered with: The same hashing function has to be applied to the received message and the resulting message digest compared with the decrypted signature (which was the message digest of the original message). If the two are the same the message is taken as being authentic.

However, how can we be sure that the sender's public key is genuine? This is where the digital certificate comes into play: The digital certificate will be sent with the original message. It includes the sender's public key, encrypted with the Certificate Authority (the trusted party)'s private key. So the recipient first has to decrypt the encrypted sender's public key using the Certificate Authority's public key.

Q13.

This question was very badly answered. Candidates rarely showed that they understood the networking protocols involved.

(a) (i) It was very disappointing to see that so many candidates do not understand the Internet. Many answers confused the Internet with the World Wide Web and there were many answers that lacked the detail required to obtain any credit. At this level candidates should be able to give a technical explanation of the Internet.

(ii) There was much confusion between the Internet and the World Wide Web. Those candidates that were able to distinguish between the two were rarely able to give a technical explanation of the Web.

(iii) Candidates often failed to obtain the mark by giving a superficial answer. Credit will not be given for stating that: "A Local Area Network is a Network in a Local Area".

(iv) As in part (iii), candidates often failed to obtain the mark by giving a superficial answer.

(v) Very few candidates understood that an Intranet is a network that provides Internet facilities within an organisation. A local area network is not an Intranet unless Internet protocols are used and few candidates were able to express this. A common misconception was that an intranet is a LAN with access to the Internet.

(b) (i) Answers to the domain name were rarely correct, often starting with http://www.

(ii) Again, there were few correct answers. Common mistakes were to give values less than 4 or values over 255.

Q14.

It was very disappointing to see how many candidates do not understand the operation of the World Wide Web. Although most candidates scored on this question very few obtained full marks.

(i) Many candidates were able to state that http is short for hypertext transfer protocol but few were able state that this is a set of rules governing data transfer.

(ii) Candidates stated that www is short for World Wide Web but few were able to state that this means that it is a web site.

(iii) Non-profit making organisation seems to be well understood.

(iv) The UK as the country of origin was well known

(v) Fewer candidates realised that this represents a directory/folder.

(vi) Although most candidates recognised this as the file name there were a sizeable minority who either concentrated on the extension or stated that it was a subdirectory of qual.

Q15.

(a) It was very disappointing to see that so many candidates do not understand the Internet. Many answers confused the Internet with the World Wide Web and there were many answers that lacked the detail required to obtain full credit. At this level computing students should be able to give a technical explanation of the Internet.

(b) Answers to the domain name were equally badly expressed. There was some understanding that a domain name was linked to an IP address. Once again candidates showed their lack of understanding of the operation of the Internet and many were confused that a domain name could only apply to the World Wide Web.

(c) Very few candidates understood that an Intranet is a network that provides Internet facilities within an organisation. A local area network is not an Intranet unless Internet protocols are used and few candidates were able to express this.

(d) Some candidates were able to identify URL as standing for uniform resource locator. Those that attempted to describe the term rarely gave sufficient detail. Once again candidates are under the impression that URL only applies to websites.

(e) Again candidates referred to the address of a web site rather than a computer or server. Many answers stated that they consist of 4 numbers but did not understand that each number is stored in one byte. As a result they failed to realise that the numbers must be in the range 0-255. They seemed to think that any 3 digit numbers will do.

Q16.

Candidates must be aware that one word answers are not usually sufficient. Just spelling out the full word from the abbreviation in the URL is enough to explain what the different parts can tell us. Particularly vague were the answers to the history part of the URL, which is a folder name of the web site. Some candidates wrongly thought it was a link. Some candidates suggested, wrongly, that each part of the URL is coded into a set of digits and this is how the IP address is arrived at. Each web site has a unique IP address. The more user-friendly domain name is resolved to its IP address through a Domain Name Server. A creditworthy response was that each domain name maps onto one IP address.

(Although it should be noted that several domain names may map onto the same IP address.) Very few candidates correctly stated the range of possible IP addresses. Many did not appear to see the significance of each group of digits being stored in one byte and therefore the possible range was 0.0.0.0 – 255.255.255.255. Some candidates were on the right track but failed to see that the largest possible integer that can be stored in a byte is 255 and stated a variety of other values. This is an important concept to understand the pending change to longer IP addresses as the world runs out of the currently available addresses.

Q17.

The majority of the candidature succeeded in making a creditable attempt at this question. The most popular answer for part (a) was the lack of any physical trace with electronic mail alterations, which is not true of alterations to paper mail. Fewer candidates answered that opportunities exist to alter emails because e-mails travel through several computers/servers to which access is possible.

Many candidates successfully deduced that a publicly distributed public key would be used to encrypt e-mail and the corresponding private key would be used to decrypt it. Some candidates failed to make it clear that the recipient's private key, not any private key, must be used. To verify that e-mail has originated from the sender and has not been altered the sender's private key can be used to encrypt the e-mail. The corresponding public key can be used to decrypt this e-mail. Many candidates understood the sequence in which the keys had to be used but fewer spelt out that decryption takes place using the sender's public key, not just any public key.

Q18.

(a) (i) Most candidates gained one or two marks here. Sharing data or the database or the need to only update a single database on the server were all answers which gained credit. However some candidates referred to Wide Area Network advantages or compared WANs and LANs, and not LAN and stand-alone operation as the question stated.

(ii) A modem appeared too frequently here. Networking, even at this quite basic level, is not a well-known topic.

(b) (i) The idea of a cable failure not taking down the whole net was reasonably well known but many candidates stated "if the Computer fails…" which did not gain credit.

(ii) Almost all candidates realised the Bus network used less cable. However, some candidates still only stated "The bus network is cheaper". Without further qualification this response did not gain credit.

(c) (i) This was very poorly answered; usually candidates only referred to an address of a site. Very few candidates understood the idea of a name of a site, which the domain name server resolves into a site address.

(ii) Most candidates gave a suitable example of a domain name, but some candidates quoted an email address, which did not gain credit. The mark scheme this year was very generous, accepting answers where candidates underlined just the company name part of a domain name, insisting that this was the domain name. Candidates need to appreciate that www.name.co.uk may belong to a different organisation than www.name.com and these are two different domain names. The whole expression is the domain name. Just as domain names can have different suffixes (such as .co.uk or .com) they can

have different prefixes such as wap. or ftp.

(d) The idea that an intranet was 'internal' or company-wide was less well known than the answer that it was 'like the Internet'. Many candidates set out their answers in terms of a LAN definition, which on its own was not enough to gain credit. Some candidates thought that the intranet consists of just one web page available to employees only. It is actually a communication system providing similar services to the Internet.

Q19.

Most candidates knew what the part of the domain meant but lost marks by expressing themselves poorly. The questions specifically asked what the different parts of a domain name could tell us, and just quoting WWW meant world wide web and the internet are the same rather than that the former is a subset of the latter. It was a pleasant surprise that so many candidates could say the domain name and IP address were mapped.

Q20.

Candidates from some centres answered this question very well and gave clear explanations of packet switching. Good answers often included an example to reinforce the explanation. Other candidates seemed less well prepared. Common errors included confusing token passing on a ring LAN with packet switching on a WAN, and answers that simply re-worded the question without any further explanation.

Q21.

This question was familiar to most candidates but the explanations often lacked sufficient detail or were too muddled to gain both marks.

Q22.

A high scoring question but a clear preference for hackers and viruses. A large number of candidates were unable to come up with a third threat.

Q23.

Many candidates made a very good attempt at this question and clearly understood the need for protocols. They often wanted to show off their knowledge in this area by giving all seven layers of the OSI seven layer model.

Q24.

This question was a rich source of marks for most candidates.

The definitions of computer viruses provided many exam howlers and provided much amusement for the examiners. Rarely were candidates prepared to consider the idea that viruses replicate without the user being aware it is happening. From the horror stories provided accessing the Internet should only be undertaken by the foolhardy since it is the main source of unknown and deadly viruses of which the most common is the millennium bug which will activate at midnight on Dec 31st 1999 - you have been warned!!!

The four groups were given in the question to help candidates come up with four distinct measures that can be taken to combat viruses. Generally this worked with candidates indicating which group they were addressing. Where candidates gave two measures appropriate to a particular group they were rewarded.

Q25.

(a) Many candidates correctly defined a wide area network as one connecting geographically remote computers or as one connecting computers spread over a large geographical area.

(b) Protocol was vaguely understood but few candidates were able to define it tightly. A protocol in the context of a wide area network is a set of rules used to define ways in which different computer networks/computers may be connected to one another. This definition was made available in material published by the Board to accompany the new syllabus.

(c) Many candidates correctly answered that without a protocol successful communication between computers could not be achieved across a wide area network. A common standard is needed because computers in a wide area network are often different.