Security

Papers Dock

COMPUTER SCIENCE 9618 PAPER 1

Security

Data Integrity

- Ensuring the accuracy and consistency of data during and after processing
- Ensuring the data is up to date.

Data Privacy

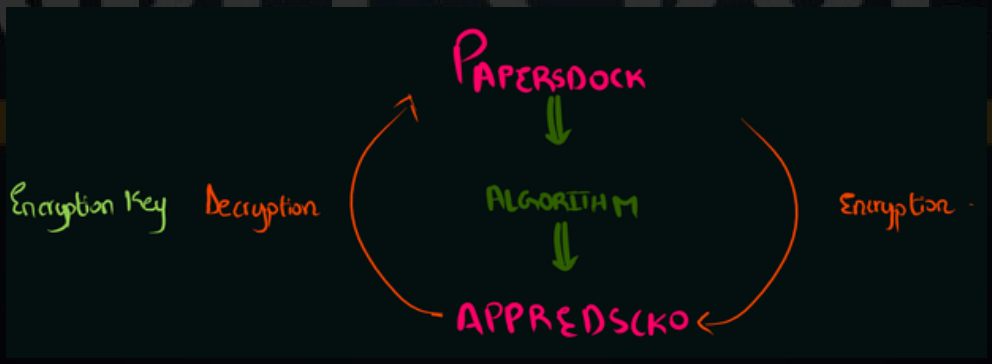
- Ensuring data can only be accessed by authorized person

Security

- Is to keep data safe
- Prevention of data loss
- e.g data backup.

Security Measures To Protect Computer

1) Encryption



- Encryption scrambles the source code
- Using an encryption key
- If the file is accessed without authorization it will be meaningless and wont me understandable
- It requires a decryption key to unscramble the algorithm.

2) Data Backup

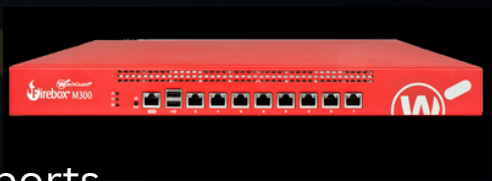
- A copy of data will have been made and stored elsewhere
- If the original data is lost, the backup can be used to restore the data.

3) Disk Mirroring

- The data is stored on two disks simultaneously
- If the first data disk drive fails, the data is accessed from the second disk.

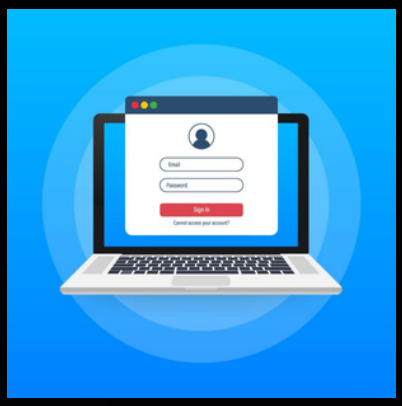
4) Firewall

- Prevents unauthorized access to the data
- Monitors incoming and outgoing traffic
- Blocks transmission from unauthorized sources/website
- Maintains an allow list
- Can be software or hardware both
- Can help to prevent hacking
- Blocks data from entering specific ports
- Blocks data that does not meet whitelist that meets blacklist



5) User Account

- User has a username and password
- Access to resources can be limited to specific account
- A person cannot access system without valid username and password.



6) Anti Malware

- Scans for malicious code (harmful code)
- Quarantines or deletes any malicious software found
- Scans can be scheduled at regular intervals.

7) Access Rights

- Different Access Rights for individual/group
- To stop users from editing program.

8) Physical Measure

- Locked doors / Keyboards
- Secure method of access

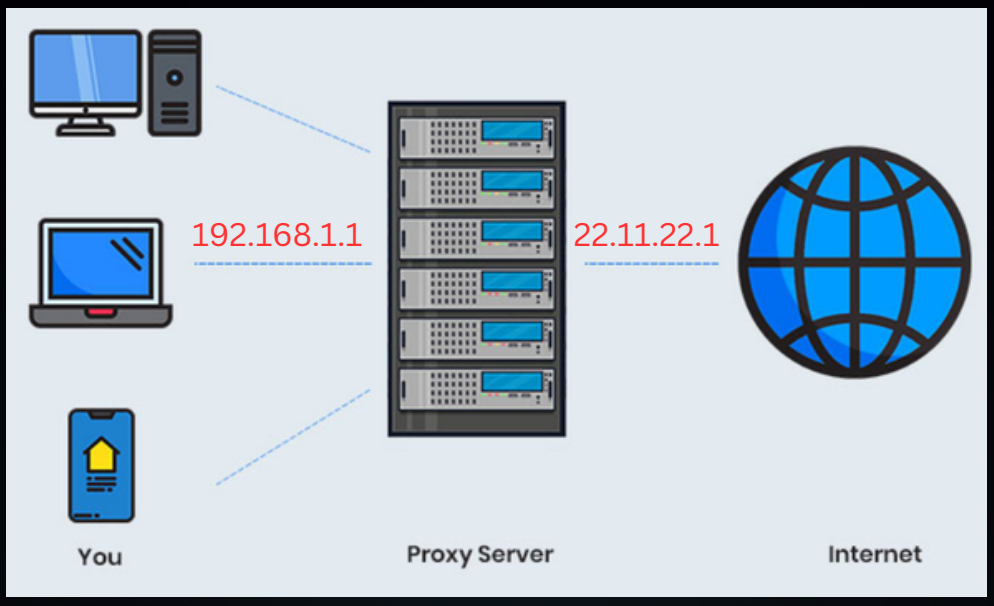
Software To Prevent Threats

Types Of Software	**Description**
Antivirus	• Scans the computer for viruses and checks against a stored database of viruses, that needs to be updated regularly and then deletes/quarantines them. • Compares downloaded files to a database of known viruses and prevents the download continuing.
Antispyware	• Scans the computer for spyware and checks against a stored database of spyware, that needs to be updated regularly and then deletes/quarantines them. • Compares downloaded files to a database of known spyware and prevents the download continuing.
Firewall	• Monitors incoming and outgoing traffic and compares it to criteria that are set by the user such as through a whitelist/blacklist or identifying allowed/blocked IP addresses. • Compares incoming and outgoing traffic to criteria and blocks those that do not match criteria.
Antimalware	• Scans the computer for viruses and checks against a stored database of viruses, that needs to be updated regularly and then deletes/quarantines them. • Compares downloaded files to a database of known viruses and prevents the download continuing.

What are the other methods to protect data online ?

- Running up to date anti virus
- Use of proxy server
- Strong biometrics / password

Proxy Server



Acts as middle man and hides
the public IP address of the user.

What are the factors to consider when planning a data backup ?

How often should the data be backed up
e.g at the end of each day as students' progress may be edited each day.

What medium should the data be backed up to
e.g external hard disk as it has larger capacity.

Where should the backup be stored
e.g off-site as if the building is damaged only the original data are lost.

What is backed up?
e.g only the updated file.

When should the backup take place?
e.g overnight.

Malware

Malware is software that is intentionally designed to cause damage to a computer or server.

Types Of Malware

Virus, Spyware

Explain the term virus ?

- Malicious Code (Harmful code)
- that replicates / copies itself
- can cause loss of data
- can cause computer to crash
- can fill up hard disk with data.

What are the ways to protect from virus ?

- Use anti-virus
- update anti-virus on regular basis
- avoids downloads from unknown sources
- use a firewall
- avoid suspicious websites.

(1) Virus

Programs or program code that can replicate itself by inserting itself into another piece of software with the intention of deleting or corrupting files.

Problem: Computer may stop working or files may get lost.

Solution: Run anti-virus software

(2) Spyware

Malware downloaded without the user's knowledge which secretly records the user's actions / keystrokes on the computer and sends logs of the actions to a third party

Solution: Anti - Spyware Software

PHISHING

The email pretends to be from an official body persuading individuals to disclose private information such as bank details or requesting authentication by redirecting to an unofficial/unauthorized website by inviting a user to click a link

Problem: Identity fraud // misuse of financial data
Solution: Ignore suspicious email and undergo frequent security awareness training.

PHARMING

Malicious code installed on user's computer or webserver. The code redirects the user to fake website.

Difference and Similarities between Phishing and Pharming

Difference:

- Pharming is malicious code that redirects to a fake website. Phishing uses an email to prompt user action.
- Pharming is automatic. Phishing requires user action.

Similarity:

- Both try to obtain financial or personal information
- Both are a false representation of an official organization, e.g. a bank
- Both make use of fake websites

Explain how the data security risks of Malware can be restricted

- Download programs from reputable websites / sources as these are less likely to contain malware
- Backup / archive computer systems so they can be restored in case of data loss from malware program installation
- Install and run anti-malware program so that regular scans can be made for known malware and if malware is found it can be quarantined / removed and computer's anti-malware definitions are regularly updated
- Using a firewall to block unused ports so that malware cannot enter the computer system
- Deny administrator privileges to everyday users so that malware cannot be downloaded by everyday users
- Avoid the use of removable devices so that malware cannot be installed from these devices

Explain why the data and computer system both should be secure from unauthorized access ?

Data

- Data needs protecting from someone amending / deleting or taking it

Computer System

- Computer system need protecting to stop people for example, installing malware or damaging the system

Data Integrity

Validation: Checks that the data entered is reasonable.
Verification: Checks that the data entered is same as the original.

Validation

Range Check: Checks whether data entered is between a lower and an upper limit
e.g. using 13 as months or -120 as age

Format Check: Checks whether data has been entered in the agreed format
e.g. format of date is dd/mm/yyyy

Length Check: Checks whether data has the required number of characters
e.g. phone number should contain 7 numbers

Presence Check: Checks to make sure a field is not left empty when it should contain data
e.g. verification code should be present

Existence Check: Checks if data in a file or a filename actually exists
e.g. registered name is found

Limit Check: Checks only one of the limits (such as the upper limit or lower limit)
e.g. 1.5 litre only.

Check Digit

Checks whether a numeric or alphanumeric identifier has been entered correctly by verifying the last digit, which is derived from the other digits using a specific algorithm.

Method for Calculating Check Digit

1. **Each digit in the number is given a weighting e.g., 7, 6, 5, 4, 3, 2, 1 starting from the left.**
2. **The digit is multiplied by its weighting and then each value is added to make a total.**
3. **The total is divided by 11 and the remainder is subtracted from 11.**

Data verification is one method of protecting the integrity of data.
Describe one other method of protecting the integrity of data ?

- **Validation**
- **protects the data by ensuring that the data is reasonable and within specified bounds**

Verification

Is a way of preventing errors when data is entered manually using a keyboard or when data is transferred from one computer to another.

Verification During Data Entry

Double Entry: Data is entered twice, and the computer compares to check they are the same

Visual Check: Entered data is compared manually with the original document

Verification During Data Transfer

Checksum: A value is calculated from the data, then appended to the end of the data. The receiver recalculates the checksum to compares the result with the value received. If the two are different, there is an error.

Parity Check: A parity bit is added to the data to ensure the number of 1s is either odd (odd parity) or even (even parity). The receiver checks the parity to detect errors.

Checksum

- bytes sent as a block
- bytes added up before transmission
- results of addition is sent with the data block
- same calculation is carried out at receiver's end
- the two values are compared.

Exam Style Question

Describe how checksum is used to detect errors during data transmission ?

- checksum value is calculated from the data before transmission
- this calculated value is transmitted with the data
- receiving computer recalculates the checksum from the received data
- if the checksum received and calculated match, no error has occurred
- if the checksum received and calculated do not match, an error has occurred

Explain why the data in the system may not be correct even after validating and verifying the data ?

- Validation checks data is reasonable/within bounds it does not check that accurate data has been entered
- Verification checks if the data matches the data given it does not check if the original data is accurate

Parity Check

Even Parity (Even number of 1's)
Odd Parity (Odd number of 1's)

5 Parity checks are often used to check for errors that may occur during data transmission.

(a) A system uses **even parity**.

Tick (✓) to show whether the following three bytes have been transmitted correctly or incorrectly.

Received byte	Byte transmitted correctly	Byte transmitted incorrectly
11001000		
01111100		
01101001		

[3]

(b) A parity byte is used to identify which bit has been transmitted incorrectly in a block of data.

The word "F L O W C H A R T" was transmitted using nine bytes of data (one byte per character). A tenth byte, the parity byte, was also transmitted.

The following block of data shows all ten bytes received after transmission. The system uses **even parity** and column 1 is the parity bit.

	letter	column 1	column 2	column 3	column 4	column 5	column 6	column 7	column 8
byte 1	F	1	0	1	0	0	1	1	0
byte 2	L	1	0	1	0	1	1	0	0
byte 3	O	1	0	1	0	1	1	1	1
byte 4	W	1	0	1	1	0	1	1	1
byte 5	C	1	0	1	0	0	0	1	1
byte 6	H	0	0	1	0	1	0	0	0
byte 7	A	0	0	1	0	0	1	0	1
byte 8	R	1	0	1	1	0	0	1	0
byte 9	T	1	0	1	1	0	1	0	0
parity byte		1	0	1	1	1	1	1	0

(i) **One** of the bits has been transmitted incorrectly.

Write the byte number and column number of this bit:

Byte number .....

Column number .....

[2]

How a parity block check can identify a bit that has been corrupted?

- Each byte has a parity bit
- An additional parity byte is sent with vertical and horizontal parity
- Each row and column must have an even/odd number of 1's
- Identify the incorrect row and column
- The intersection is the error.

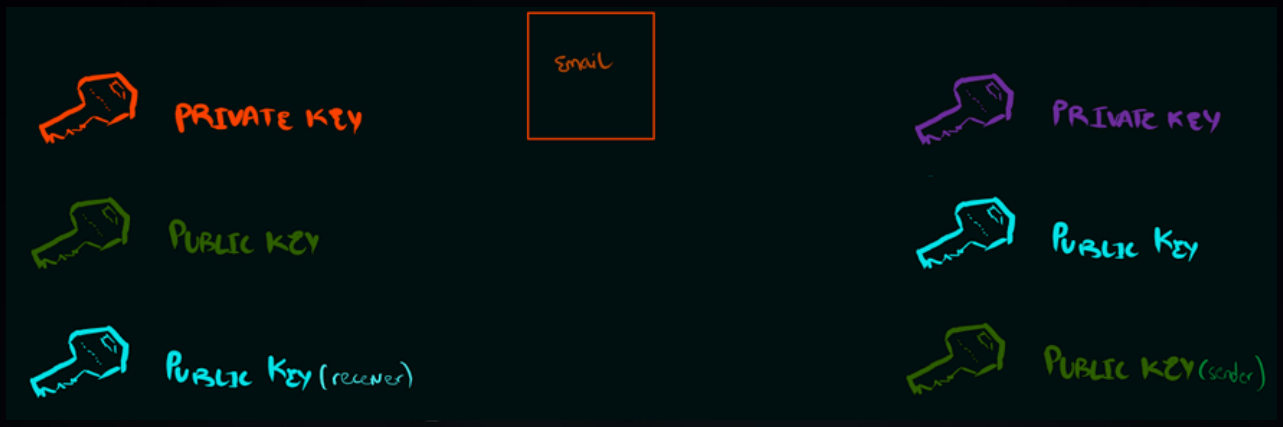
Computer A and Computer B agree on whether to use odd or even parity.
Computer A divides the data into groups of 7-bits. The number of 1s in each group is counted. If the agreed parity is odd and the group has an even number of 1s a parity bit of 1 is appended, otherwise, a parity bit of 0 is appended.

In a parity block check the bytes are grouped together, for example in a grid. The number of 1s in each column (bit position) is counted. A bit is assigned to each column to make the column match the parity. These parity bits are transmitted with the data as a parity byte.

State the difference between data verification and data validation ?

data verification is checking if input data is the same as the original whereas data validation is checking that the data is reasonable / sensible

Digital Signature



Hashing Algorithm

Hashing algorithms are mathematical functions that produce a hash key.

Explain how digital signature is used to ensure email is authentic?

- Email message put through hashing algorithm to produce a digest.
- Digest is encrypted with sender's private key to create digital signature.
- The digital signature can only be decrypted with matching sender’s public key.

Explain how a digital signature is used to authenticate a digital document during transmission over a network?

- The sender hashes the document
- to produce a digest
- The sender encrypts the digest to create the digital signature
- The message and the signature are sent to the receiver
- The receiver decrypts the signature to reproduce the digest
- The receiver uses the same hashing algorithm on the document received to produce a second digest
- The receiver compares this digest with the one from the digital signature
- If both of the receiver's digests are the same, the document is authentic

Security, privacy and data integrity

Question 1

6 Each of the following algorithms performs data validation.

State the type of validation check that each of the algorithms performs.

(a)

```
INPUT x
IF x < 0 OR x > 10 THEN
  OUTPUT "Invalid"
ENDIF
```

..... [1]

(b)

```
INPUT x
IF x = "" THEN
  OUTPUT "Invalid"
ENDIF
```

..... [1]

(c)

```
INPUT x
IF NOT(x = "Red" OR x = "Yellow" OR x = "Blue") THEN
  OUTPUT "Invalid"
ENDIF
```

..... [1]

Question 2

8 A company has several security measures in place to prevent unauthorised access to the data on its computers.

(a) Describe the difference between the security and privacy of data.

.....

.....

.....

..... [2]

(b) Each employee has a username and password to allow them to log onto a computer. An employee's access rights to the data on the computers is set to either read-only, or read and write.

Identify **one** other software-based measure that could be used to restrict the access to the data on the computers.

.....

..... [1]

(c) The company is also concerned about threats posed by networks and the internet.

Identify **two** threats to the data that are posed by networks and the internet.

Threat 1 .....

.....

Threat 2 .....

.....

[2]

Question 3

2 Xanthe wants to maintain the integrity and security of data stored on her computer.

(a) Explain the difference between data security and data integrity.

.....

.....

.....

..... [2]

(b) Xanthe uses both data validation and data verification when entering data on her computer.

(i) Describe how data validation helps to protect the integrity of the data. Give an example in your answer.

Description .....

.....

.....

Example .....

[2]

(ii) Describe how data verification helps to protect the integrity of the data. Give an example in your answer.

Description .....

.....

.....

Example .....

[2]

(c) Two malware threats are spyware and viruses.

Give **two** similarities and **one** difference between spyware and a virus.

Similarity 1 .....

.....

Similarity 2 .....

.....

Difference .....

.....

[3]

Question 4

1 When designing computer systems, it is important to consider the security, integrity and privacy of the data.

Draw **one** line from each measure to indicate whether it keeps data secure or protects the integrity of data.

Measure

Firewall	
Double entry	Data Security
Presence check	
Access rights	Data Integrity
Password	

[2]

Question 5

3 A teacher is writing examination papers on a laptop computer. The computer is connected to the internet. The teacher is concerned about the security and privacy of the papers.

(a) State the difference between the security of data and the privacy of data.

.....

.....

..... [1]

(b) Identify **and** describe **two** threats to the data. Identify **one** security measure to protect against each threat. Each security measure must be different.

Threat 1 .....

Description .....

.....

Security measure .....

Threat 2 .....

Description .....

.....

Security measure .....

[6]

Question 6

(d) The mark a student is awarded in a test will be entered into the database. This mark needs to be a whole number between 0 and the maximum number of marks for that test (inclusive).

Explain how data validation **and** data verification can be used when a mark is entered.

.....

.....

.....

.....

.....

.....

.....

..... [4]

Question 7

4 A school stores personal data about its staff and students on its computer system.

(a) Explain why the school needs to keep both its data **and** its computer system secure from unauthorised access.

Data .....

.....

Computer system .....

.....

[2]

(b) Complete the table by identifying **two** security threats to the data on a computer.

Describe each threat.

Give a different prevention method for each threat.

Threat	Description	Prevention method
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....

[6]

(c) Data is encrypted when it is transmitted within the school network, or externally such as over the internet.

Describe what is meant by encryption **and** explain why it is used.

.....

.....

.....

..... [2]

Question 8

5 A company wants to store data about its employees in a computer system. The owner of the company wants to ensure the security and integrity of the data.

(a) **(i)** State why data needs to be kept secure.

.....

..... [1]

(ii) One way the data stored in a computer can be kept secure is by using back-up software.

Give **two other** ways the data stored in a computer can be kept secure.

1 .....

.....

2 .....

..... [2]

(b) The data about the employees is currently stored on paper. The data needs to be transferred into the computer system.

Data validation and verification are used to help maintain the integrity of the data.

(i) Identify **and** describe **one** method of data verification that can be used when transferring the data from paper to the computer.

Method .....

Description .....

.....

..... [2]

(ii) The company needs to transfer the date of birth of each employee into the computer system.

Give **one** example of how each of the following data validation rules can be used to validate the date of birth when it is entered into the system.

Range check .....

.....

Presence check .....

.....

Length check .....

.....

[3]

(iii) Explain why the data in the system may **not** be correct even after validating and verifying the data.

.....

.....

.....

.....

.....

..... [2]

Question 9

2 Draw **one** line from each security feature to its most appropriate description.

Security feature	Description
firewall	converts data to an alternative form
pharming	redirects a user to a fake website
anti-virus software	verifies the authenticity of data
encryption	scans files on the hard drive for malicious software
	accepts or rejects incoming and outgoing packets based on criteria

[4]

Question 10

4 **(a)** State the difference between **data verification** and **data validation**.

.....

.....

..... [1]

(b) A checksum can be used to detect errors during data transmission.

Describe how a checksum is used.

.....

.....

.....

.....

.....

..... [3]

(c) One validation method is a presence check.

Describe **two other** validation methods that can be used to validate non-numeric data.

1 .....

.....

2 .....

.....

[2]

Question 11

6 **(a)** A student uses a networked laptop computer to send an email to a colleague.

(i) Explain how a digital signature ensures the email is authentic.

.....

.....

.....

..... [2]

(ii) Describe how a firewall protects the data on the computer.

.....

.....

.....

.....

.....

..... [3]

Question 12

(c) The database `Lessons` has the following tables:

`HORSE(HorseID, Name, Height, Age, HorseLevel)`

`STUDENT(StudentID, FirstName, LastName, RiderLevel, PreferredHorseID)`

`LESSON(LessonID, Date, Time, StudentID, HorseID, LessonContent)`

Dates in this database are stored in the format `#DD/MM/YYYY#`.

The fields `RiderLevel` and `HorseLevel` can only have the values: `Beginner`, `Intermediate` or `Advanced`.

(i) Describe **two** methods of validating the field `RiderLevel`.

1 .....

.....

.....

2 .....

.....

.....

[2]

Question 13

(d) The data is validated and verified when it is entered into the database.

(i) The car registration number must be: 1 letter, followed by 3 numbers, followed by 2 letters.

For example, A123AA is valid but A12AA is invalid.

One way that a registration number can be validated is by using a presence check to make sure the registration number has been entered.

Describe **two other** ways that the car registration number can be validated.

1 .....

.....

2 .....

.....

[2]

(ii) Describe **two** ways that the car registration number can be verified when it is entered into the database.

1 .....

.....

2 .....

.....

[2]

(iii) State why the car registration number might be incorrect even after it has been validated and verified.

.....

..... [1]

Question 14

6 Data needs to be kept secure when stored on a computer and during transmission over a network.

(a) Explain how a digital signature is used to authenticate a digital document during transmission over a network.

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [5]

(b) Complete the table by identifying **and** describing **two** types of software that can be installed on a computer to prevent threats over a network.

Type of software	Description
.....	.....
.....	.....
	.....
.....	.....
.....	.....
	.....

[2]

Question 15

5 **(a)** State the meaning of **privacy of data**.

.....

..... [1]

(b) State the meaning of **integrity of data**.

.....

..... [1]

(c) Describe the following threats to a computer system.

Phishing email .....

.....

.....

.....

Spyware .....

.....

.....

.....

[4]

Question 16

8 **(a)** Data verification is one method of protecting the integrity of data.

Describe **one** other method of protecting the integrity of data.

.....

.....

.....

..... [2]

(b) State **one** difference and **one** similarity between pharming and phishing.

Difference .....

.....

Similarity .....

.....

[2]

(c) Explain how the data security risks of malware can be restricted.

.....

.....

.....

.....

.....

..... [3]

Question 17

(b) The bank wants to protect the integrity of its data while transferring the data to other banks. Parity check is one example of data verification.

Complete the description of parity check when Computer A is transmitting data to Computer B.

Computer A and Computer B agree on whether to use ..... parity. Computer A divides the data into groups of ..... . The number of 1s in each group is counted. If the agreed parity is ..... and the group has an even number of 1s, a parity bit of 1 is appended, otherwise a parity bit of 0 is appended.

In a parity ..... check the bytes are grouped together, for example in a grid. The number of 1s in each column (bit position) is counted. A bit is assigned to each column to make the column match the parity. These parity bits are transmitted with the data as a parity ..... .

[5]

(c) The bank also needs to keep its customers' data private and secure.

(i) The bank's network has a firewall.

Explain how a firewall can help protect the customers' data.

.....

.....

.....

.....

.....

.....

.....

..... [3]

Question 18

3 An assessment board scans exam papers and stores the digitised papers on a server. Exam markers download the digitised papers to mark. The exam markers then upload the mark for each paper.

(a) The assessment board needs to make sure the data stored on the server is secure.

(i) Authentication methods can help to protect the server against hackers.

Identify **one other** security measure that helps to protect the server from hackers.

Describe how the security measure works.

Security measure .....

Description .....

.....

.....

.....

[3]

(ii) Identify **one** security measure that helps to protect the data when it is being transmitted to its destination. Describe how the security measure works.

Security measure .....

Description .....

.....

.....

.....

[3]

Question 19

(f) The data from the robots is transmitted to a central computer using a wireless connection.

(i) Complete the table by identifying **and** describing **two** methods of data verification that can be used during data transfer.

	Method	Description
1	.....	.....
	.....	.....
	.....	.....
		.....
		.....
		.....
2	.....	.....
	.....	.....
	.....	.....
		.....
		.....
		.....

[4]

(ii) Explain how encryption can protect the security of data during transmission.

.....

.....

.....

..... [2]

9608 Topical Past Paper

Question 20

A computer program makes use of data validation routines and verification of data input.

(a) Complete these two sentences about data validation and verification.

1. ..... checks that the data entered is reasonable. One example is ..... .

2. ..... checks that the data entered is the same as the original. One example is ..... . [4]

(b) The program is installed on a computer system that has security measures in place to protect its data.

Security measure	Description
....	Data are written on two or more disks simultaneously.
Encryption	....
....	A copy of the data is taken and stored in another location.

[3]

Question 21

(d) The company needs to keep the data on its servers secure from online threats.

(i) Describe how a firewall will help to protect the data on the servers from online threats.

.....

.....

.....

.....[2]

(ii) Give one additional security measure that the company can use to protect the data on the servers from online threats.

..... [1]

Question 22

(a) He wants to make sure the source code is secure on his laptop. Explain how encrypting the source code can keep it secure.

.....

.....

.....

.....

.....

..... [3]

Question 23

(b) The software development company uses data backup and disk-mirroring to keep their data secure. Explain how data backup and disk-mirroring allow the company to recover from data loss.

Data backup .....

.....

.....

.....

Disk-mirroring .....

.....

.....

.....[4]

Question 24

Frankie is a software developer. He is developing a program to manage customer records for a client with an online retail business. He must ensure that data stored about each customer are both secure and private.

(a) State the difference between security and privacy.

.....

.....

.....

..... [2]

(b) Computer systems can be protected by physical methods such as locks. Describe two non-physical methods used to improve the security of computer systems.

1 .....

.....

.....

.....

.....

.....

2 .....

.....

.....

.....

.....

..... [6]

(c) A computer uses parity blocks to check the data that has been received is the same as the data that has been transmitted.

The following is an example of a parity block.

	Parity bit	Data						
	1	1	1	1	0	0	0	1
	0	0	0	0	1	1	1	0
	1	1	0	1	1	0	0	1
Parity byte	1	1	0	1	1	0	0	1

(i) Describe how a parity block check can identify a bit that has been corrupted during transmission.

.....

.....

.....

.....

.....

.....

.....

..... [4]

(ii) Give a situation where a parity block check cannot identify corrupted bits.

.....

..... [1]

Question 25

ii) The supermarket is concerned about the security and integrity of the data on the server. Identify two methods that can be used to minimise the security risk to the data, and one method to protect the integrity of the data.

Security 1 .....

.....

Security 2 .....

.....

Integrity .....

..... [3

Question 26

6 Parity bits can be used to verify data.

(a) The following binary number is transmitted using **even** parity.

Add the missing parity bit.

Parity bit							
	1	0	1	1	0	1	0

[1]

(b) In the following parity block, the first column contains the parity bits, and the last row contains the parity byte. A device transmits the data using **even** parity.

(i) Circle the error in the data transmitted.

	Parity bit	Data						
	1	1	0	1	0	1	1	1
	1	0	0	0	1	1	1	0
	0	1	0	0	1	0	1	1
	1	1	1	0	1	1	1	1
Parity byte	1	1	1	1	1	0	0	1

[1]

(ii) Explain how you identified the error.

.....

.....

.....

.....

.....[2]

(c) The data received can contain errors that are not detected using parity bits.

Explain how this can happen.

.....

.....

.....

.....[2]

(d) Parity is not the only method to verify the data has been sent correctly. Name and describe one other method of data verification during data transfer.

Name .....

Description .....

.....

.....

.....

.....

..... [3

Question 27

3 Parity bits can be used to verify data.

(a) The following binary number is transmitted using **odd** parity.

Add the missing parity bit.

Parity bit							
	0	1	0	0	0	0	0

[1]

(b) In the following data transmitted, the first column contains the parity bits, and the last row contains the parity byte. A device transmits the data using **even** parity.

Circle the error in the data transmitted.

	Parity bit	Data						
	1	0	1	0	1	1	1	1
	0	1	1	0	0	1	1	0
	1	1	0	0	0	0	0	0
	0	1	0	0	0	0	0	0
Parity byte		0	0	0	0	1	0	0	1

[1]

(c) The following table shows five error detection measures.

Put **one** tick (✓) in each row to indicate whether the measure is validation or verification.

Measure	Validation	Verification
Checksum		
Format check		
Range check		
Double entry		
Check digit		

[5]

Question 28

Parity bits can be used to verify data.

(a) The following binary number is transmitted using **odd** parity.

Add the missing parity bit.

Parity bit							
	0	1	1	1	0	1	0

[1]

(b) In the following parity block, the first column contains the parity bits, and the last row contains the parity byte. A device transmits the data using **even** parity.

Circle the error in the data being transmitted.

	Parity bit	Data						
	0	0	1	1	0	1	0	1
	1	1	1	1	1	0	0	1
	1	0	1	0	1	0	0	0
	0	0	0	1	1	0	1	1
Parity byte	0	1	1	1	1	1	0	1

[1]

(c) Four error detection measures are shown.

Draw **one** line from each error detection measure to indicate whether it is verification or validation.

Error detection measure

Type check	
Proof reading	Verification
Check digit	Validation
Checksum	

[4]

Question 29

A computer receives data from a remote data logger. Each data block is a group of 8 bytes.
A block is made up of seven data bytes and a parity byte.

Each data byte has a parity bit using odd parity. The parity byte also uses odd parity.

The following table shows a data block before transmission. Bit position 0 is the parity bit.

Bit position							
7	6	5	4	3	2	1	0
1	1	0	0	1	1	0	1
0	0	1	0	0	0	0	0
1	0	0	1	1	1	0	**A**
1	1	0	0	0	0	1	0
1	1	0	0	0	0	1	0
1	1	0	0	0	1	1	**B**
0	0	0	0	0	0	0	0

Data bytes

0	1	1	0	1	1	0	0

← Parity byte

(a) (i) Describe how the data logger calculates the parity bit for each of the bytes in the data block.

.....

.....

.....[2]

(ii) State the two missing parity bits labelled A and B.

A = ...

B = ... [1]

(iii) Describe how the computer uses the parity byte to perform a further check on the received data bytes. .....

.....

.....[2]

(b) (i) A second data block is received as shown in the following table. There are errors in this data block.

Identify and then circle **two** bits in the table which must be changed to remove the errors.

Bit position							
7	6	5	4	3	2	1	0
1	0	0	0	1	1	0	0
0	0	1	0	0	0	0	0
0	0	1	1	0	1	0	1
1	1	1	1	0	0	0	1
1	1	0	0	0	0	1	0
0	0	1	0	0	1	0	0
0	0	0	0	0	0	0	1

0	1	0	1	1	0	0	0

[2]

(ii) Explain how you arrived at your answers for part (b)(i).

.....

.....

.....

.....[3]

Question 30

A Local Area Network is used by staff in a hospital to access data stored in a Database Management System (DBMS). (a) Name two security measures to protect computer systems.

1 .....

2 ..... [2]

(b) A frequent task for staff is to key in new patient data from a paper document. The document includes the patient's personal ID number. (i) The Patient ID is a seven digit number. The database designer decides to use a check digit to verify each foreign key value that a user keys in for a Patient ID. When a user assigns a primary key value to a Patient ID, the DBMS adds a modulus-11 check digit as an eighth digit. The DBMS uses the weightings 6, 5, 4, 3, 2 and 1 for calculating the check digit. It uses 6 as the multiplier for the most significant (leftmost) digit.

Show the calculation of the check digit for the Patient ID with the first six digits 786531.

Complete Patient ID .....[4]

(ii) Name and describe two validation checks that the DBMS could carry out on each primary key value that a user keys in for a Patient ID.

1 Validation check .....

Description .....

.....

2 Validation check .....

Description .....

..... [4]

Question 31

A Local Area Network is used by school staff who access data stored in a Database Management System (DBMS).

(a) (i) Explain the difference between security and privacy of data.

.....

.....

.....

.....

.....

..... [3]

(ii) Give an example for this application where privacy of data is a key concern.

.....

.....[1]

(b) Name and describe two security measures the Network Manager has in place to protect the security of the data held in the DBMS.

1 .....

.....

.....

.....

2 .....

.....

.....

..... [4]

(c) A task for staff at the start of the school year is to key in new pupil data from a paper document. The data is entered to a screen form and includes the data verification of some fields.

Describe what is meant by verification.

.....

.....

.....

.....[2]

Question 32

5 **(a)** A Database Management System (DBMS) provides the following features.

Draw a line to match each feature with its description.

Feature	Description
Data dictionary	A file or table containing all the details of the database design
Data security	Data design features to ensure the validity of data in the database
Data integrity	A model of what the database will look like, although it may not be stored in this way
	Methods of protecting the data including the uses of passwords and different access rights for different users of the database

[3]

A school stores a large amount of data that includes student attendance, qualification and contact details. The school is setting up a relational database to store these data.

(b) The school needs to safeguard against any data loss.

Describe three factors to consider when planning a backup procedure for the data.

Justify your decisions.

1 .....

.....

.....

2.....

.....

.....

3.....

.....

.....6]

Question 33

A bank holds personal data about its customers and their financial data.

(a) Describe the difference between security and integrity of data.

.....

.....

.....

.....

.....

.....

.....

.....[4]

(b) Describe three security measures that the bank could implement to protect its electronic data.

Security measure 1 .....

Description .....

.....

.....

Security measure 2 .....

Description .....

.....

.....

Security measure 3 .....

Description .....

.....

.....[6]

Question 34

(c) Employees using the new computers receive training. At the end of the training, each employee completes a series of questions.

Three answers given by an employee are shown below.

Explain why each answer is incorrect.

(i) "Encryption prevents hackers breaking into the company's computers."

.....

.....

.....

.....[2]

(ii) "Data validation is used to make sure that data keyed in are the same as the original data supplied."

.....

.....

.....

.....[2]

(iii) "The use of passwords will always prevent unauthorised access to the data stored on the computers"

.....

.....

.....

.....[2]

Question 35

(a) Give the definition of the terms firewall and authentication. Explain how they can help with the security of data.

Firewall .....

.....

.....

.....

.....

.....

Authentication .....

.....

.....

..... [3]

(b) Describe two differences between data integrity and data security.

.....

.....

.....

.....

.....

..... [2]

(c) Data integrity is required at the input stage and also during transfer of the data.

(i) State two ways of maintaining data integrity at the input stage. Use examples to help explain your answer.

.....

.....

.....

.....

.....

..... [3]

(ii) State two ways of maintaining data integrity during data transmission. Use examples to help explain your answer.

.....

.....

.....

.....

.....

..... [3]

Question 36

(a) Give a brief description of each of the following terms:

Validation .....

.....

.....

Verification .....

.....

.....[2]

(b) Data are to be transferred between two devices. Parity checks are carried out on the data.

Explain what is meant by a parity check. Give an example to illustrate your answer.

.....

.....

.....

.....

.....

.....

.....

.....

..... [4]

Question 37

(a) Explain the term computer virus.

.....

.....

.....

.....[2]

(b) A virus checker has been installed on a PC.

Give two examples of when a virus checker should perform a check.

1 .....

.....

2 .....

..... [2]

Question 38

7 **(a)** The string of characters, "BINARY CODE", was transmitted using 11 bytes of data. An additional byte, called the parity byte, was also transmitted.

Parity bytes can be used to identify exactly which bit has been transmitted incorrectly.

The table shows bit patterns for all 12 bytes after transmission. Even parity was used and the first bit is the parity bit.

	character	bit 1	bit 2	bit 3	bit 4	bit 5	bit 6	bit 7	bit 8
byte 1	B	0	1	0	0	0	0	1	0
byte 2	I	1	1	0	0	1	0	0	1
byte 3	N	0	1	0	0	1	1	1	0
byte 4	A	0	1	0	0	0	0	0	1
byte 5	R	1	1	0	1	0	0	1	0
byte 6	Y	0	1	1	1	1	0	0	1
byte 7		1	0	1	0	0	0	0	0
byte 8	C	1	1	0	0	0	0	1	1
byte 9	O	1	1	0	0	1	1	1	1
byte 10	D	0	1	0	0	0	1	0	0
byte 11	E	1	1	0	0	0	1	0	1
parity byte		0	0	1	0	0	0	1	0

(i) There is one error in the transmission.

Indicate the byte number and bit number of the bit which has been incorrectly transmitted.

Byte number .....

Bit number .....[2]

(ii) Explain your answer to part (i).

.....

.....

.....

.....[2]

(b) Verification and validation can be applied during data entry.

Describe what is meant by these terms. For each method, explain why it is needed.

Verification .....

.....

.....

.....

Validation .....

.....

.....

.....[4]

Question 39

(a) A communication line uses half duplex.

State what is meant by half duplex.

.....

..... [1]

(b) A computer system uses **even parity**. The leftmost position of each byte is the parity bit.

(i) Complete the byte below:

	1	0	1	0	0	0	1

[1]

(ii) The parity bit is used to perform a parity check when a byte is transmitted from computer **A** to computer **B**.
Explain how computer **B** will establish whether or not the byte has been transmitted correctly.

.....

.....

.....

..... [2]

(c) In addition to a parity bit check on a byte, a parity block check is also carried out. Computer **A** transmits four bytes followed by a parity byte. The following sequence of bytes has just been received by computer **B**.

```
1 0 1 1 0 1 1 1
0 1 1 1 1 0 0 0
0 0 0 1 1 0 1 0
0 1 1 1 0 0 0 1
-----------------
1 0 1 0 1 1 0 0  <-- parity byte
-----------------
```

One of the four bytes has an error in one of the bits.

(i) Identify the byte where the error has occurred with an arrow.
Circle the bit that has been altered. [2]

(ii) Write down the corrected byte:

[1]

(iii) Explain what the computer system needs to do if more than 1 bit has been transmitted wrongly.

.....

.....

.....

..... [2]

Question 40

(a) What is meant by a computer virus?

.....

.....

.....[1]

(b) It is important to protect a computer system from viruses.

Describe **three** different ways to do this.

1 .....

.....

.....

2 .....

.....

.....

3 .....

.....

.....[3]

Question 41

(b) The word ***C O M P U T I N G*** is to be transmitted as nine bytes of data. Each character in the word has an ASCII value.

The system uses even parity and the left most bit is added to make each byte even parity.

(i) Complete the codes so that they all have even parity.

C		1	0	0	0	0	1	1
O		1	0	0	1	1	1	1
M		1	0	0	1	1	0	1
P		1	0	1	0	0	0	0
U		1	0	1	0	1	0	1
T		1	0	1	1	0	0	0
I		1	0	0	1	0	0	1
N		1	0	0	1	1	1	0
G		1	0	0	0	1	1	1

[2]

(ii) Fill in the parity byte in the final row in the table above. [1]

(iii) The character '**P**' is received incorrectly as **0 1 0 1 1 0 0 0**

Describe how horizontal and vertical parity checking would be used to detect the erroneous bit.

.....

.....

.....

.....

.....

..... [3]

Question 42

The term **L O G I C G A T E S** is to be transmitted as 12 bytes of data.

Each character in the term has an ASCII value. The system is using ***odd parity*** and the left-most bit is used as the parity bit. An additional parity byte is also sent after the term.

The following bytes arrived at their destination:

		1	2	3	4	5	6	7	8
	letters	bytes received							
1	L	0	1	0	0	1	1	0	0
2	O	0	1	0	0	1	1	1	1
3	G	1	1	0	0	0	1	1	1
4	I	0	1	0	0	1	0	0	1
5	C	0	1	0	0	0	0	1	1
6	<Space>	0	0	1	1	0	0	1	0
7	G	1	1	0	0	0	1	1	1
8	A	1	1	0	0	0	1	0	1
9	T	0	1	0	1	1	0	0	0
10	E	0	1	0	0	0	1	0	1
11	S	0	1	0	1	0	1	1	1
12	parity byte	0	1	0	0	1	1	1	1

(a) One of the bytes has an error after transmission.

(i) Locate which character contains the error.

..... [1]

(ii) Indicate which bit has been transmitted incorrectly.

column number .....

row number ..... [1]

(iii) Explain how you arrived at your conclusion.

.....

.....

.....

.....

.....

.....

..... [3]

(b) The following bytes were sent during a data transmission:

0 0 1 1 0 0 0 1
1 0 0 1 1 0 1 1
1 1 1 0 0 0 0 0

Explain how a checksum is used to check whether the bytes have been corrupted during data transmission.

.....

.....

.....

.....

.....

.....

..... [3]

Answer

Answer 1

6(a)	Range (check)	**1**
6(b)	Presence (check)	**1**
6(c)	Existence (check)	**1**

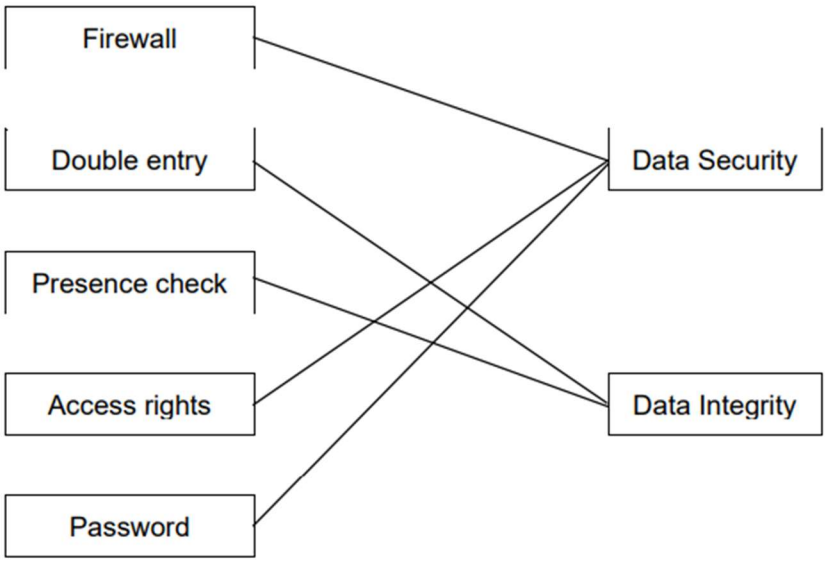
Answer 2

8(a)	**1 mark** per bullet point • Security protects data against loss • Privacy protects data against unauthorised access	**2**
8(b)	**1 mark** for a correct answer • Two factor authentication • Biometric passwords • Key Card Access • Firewall	**1**
8(c)	**1 mark** per correct answer to **max 2** • Malware // viruses // spyware // by example • Hacking • Phishing • Pharming	**2**

Answer 3

2(a)	**1 mark** per bullet point • security is protecting data from loss / corruption • integrity is ensuring the consistency / accuracy of the data	**2**
2(b)(i)	**1 mark** per bullet point • validation checks that data is reasonable / sensible • example e.g. checking data is the right number / type of characters	**2**
2(b)(ii)	**1 mark** per bullet point • verification checks that data is the same as the original • by example e.g. double entry	**2**
2(c)	**1 mark** per similarity to **max 2** • Both are pieces of malicious software • Both are downloaded / installed/run without the user's knowledge • Both can pretend to be / are embedded in other legitimate software when downloaded // both try to avoid the firewall • Both run in the background **1 mark** for difference • Virus can damage computer data; spyware only records / accesses data • Virus does not send data out of the computer; spyware sends recorded data to third party • Virus replicates itself; spyware does not replicate itself	**3**

Answer 4

1	**1 mark** for 3 correct lines only from Data Security **1 mark** for 2 correct lines only from Data Integrity 	**2**

Answer 5

3(a)	Security prevents against **loss** while privacy prevents **unauthorised access**	**1**
3(b)	**1 mark** for identifying threat, **1 mark** for description, **1 mark** for security measure (**times 2**) e.g. • Malware • Malicious software that replicates and can delete/damage the examination papers • Install and run anti-malware • Hacker/unauthorised access • Illegal access in order to delete/damage the examination papers • Use a firewall // strong passwords • Spyware • Software installed on the computer without the teacher's knowledge which records keystrokes and sends the data gathered about the examination papers to a third party • Use a firewall / install and run anti-spyware / use a virtual (onscreen) keyboard	**6**

Answer 6

4(d)	**1 mark** per bullet point to **max 3** for validation e.g. • **range check** to make sure it is between 0 and max marks • **presence check** to make sure a mark is entered • **type check** to make sure an integer value is entered **1 mark** per bullet point to **max 2** for verification e.g. • double entry - enter the mark twice and **the computer** compares them • visual check – **manually** compare the mark entered with the mark on the input document	**4**

Answer 7

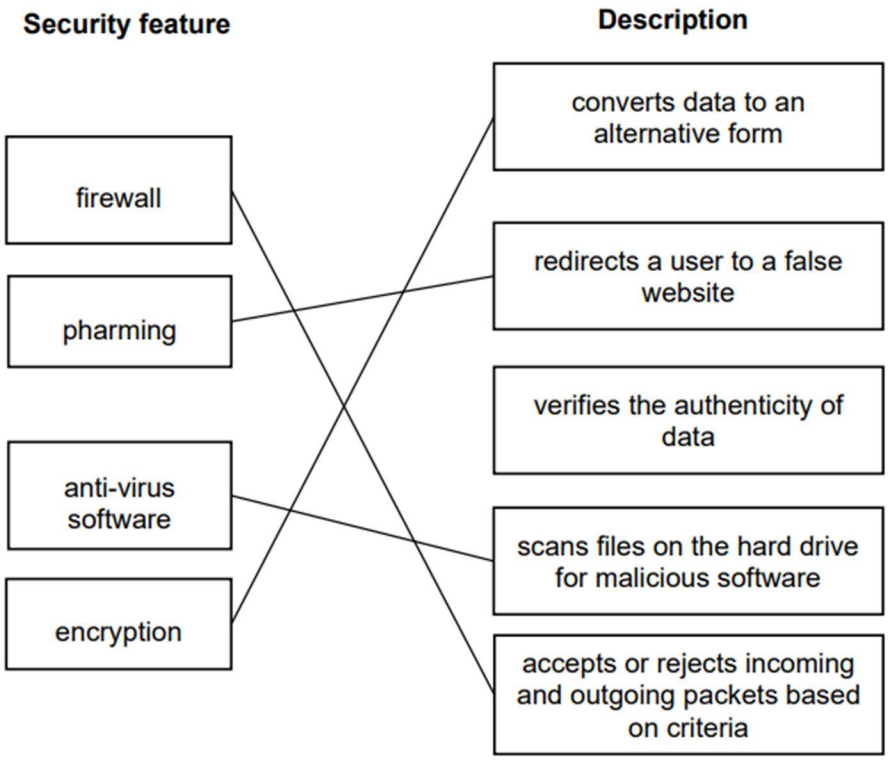
4(a)	**1 mark** per point, **max 1** for data and **max 1** for computer system Data • Data needs protecting from someone **amending / deleting** or **taking** it Computer System • Computer system need protecting to stop people for example, installing malware or damaging the system	**2**
4(b)	**1 mark** for each correct threat, matching description and prevention e.g.	**6**
4(c)	**1 mark** per point to **max 2** • Data is turned into <u>cipher text</u> // Data is **encoded** • Used so that it cannot be **understood** if intercepted **without the decryption key**	**2**

Threat	Description	Prevention method
Virus	**Malicious software** that replicates itself and can corrupt data	Anti-virus / Firewall / Anti-malware
Hacker	Unauthorised access to the computer **with** malicious **intent**	Firewall / **strong** or biometric passwords / user permissions

Answer 8

5(a)(i)	**1 mark** from • To stop the data being lost / corrupted / amended • To make sure it can be recovered • To prevent unauthorised access	**1**
5(a)(ii)	**1 mark** each e.g. • Install / run a firewall • **Up to date** Anti-virus / anti-malware • (Username and**)** **(**strong) password • Encryption • Access rights	**2**
5(b)(i)	**1 mark** each • Visual check • **Manually** compare the data entered with the original (document) • Double entry • Enter the data twice and **the system** compares them to see if they are the same	**2**
5(b)(ii)	**1 mark** each e.g. Range check: • Make sure it is after and before a specific date // e.g. between 1900 and today's date // check month is between 1 and 12 // check day is between 1 and month end Presence check: • Make sure the date of birth has been entered Length check: • Make sure there are at least 1 for day, 1 for month, 2/4 for year // must be 8 characters	**3**
5(b(iii)	1 mark per bullet point to **max 2** • Validation checks data is reasonable/within bounds it does not check that accurate data has been entered • Verification checks if the data matches the data given it does not check if the **original** data is accurate	**2**

Answer 9

2	**1 mark** for each correct line. 	**4**

Answer 10

4(a)	data verification is checking if input data is the same as the original whereas data validation is checking that the data is reasonable / sensible	**1**
4(b)	**1 mark** for each bullet point **(max 3)**: • checksum value is calculated **from the data** before transmission // correct description of a checksum algorithm • ... this calculated value is transmitted with the data • **receiving** computer recalculates the checksum from the received data • if the checksum **received** and **calculated** match, no error has occurred // if the checksum **received** and **calculated** do not match, an error has occurred	**3**
4(c)	**1 mark** for each bullet point **(max 2)**. For example: • to make sure data is in the required format // only expected characters allowed • to make sure the data is already present in the system • to make sure the data contains the correct number of characters • to ensure that non-numeric data is entered	**2**

Answer 11

6(a)(i)	**1 mark** for each method of ensuring authenticity **(max 2)**: • (email) message put through hashing algorithm to produce a digest • Digest encrypted with sender's private key (to create the digital signature) • the (digital) signature can **only** be decrypted with matching sender's public key	**2**
6(a)(ii)	**1 mark** for each bullet point: • **monitors** incoming and outgoing packets / traffic • **checks against** an allow list / deny list of IP addresses // **checks against** a set of rules for acceptable data / ports etc. • **blocks** transmissions that do not meet criteria / rules // **allows** through is satisfies the criteria /rules	**3**

Answer 12

2(c)(i)	**1 mark** each to **max 2** • Presence check to make sure that the (rider level) is entered • Look-up / Existence check to make sure the rider level is only Beginner, Intermediate or Advanced • Length check to make sure the rider level entered is either 8 or 12 characters • Type check to make sure the rider level is alphanumeric	**2**

Answer 13

4(d)(i)	**1 mark** each to **max 2** • Length check: the registration number must be **6 characters** long • Format check: the registration number must be in the format **letter-digit-digit-digit-letter-letter** • Type check: the registration number must be **alphanumeric**	**2**
4(d)(ii)	**1 mark** each • Visual check: **Manually** compare the registration number entered with the source document • Double entry: Enter the registration number twice and **the computer compares** to check they are the same	**2**
4(d)(iii)	The registration number on the original document might be in the correct format but may be the incorrect registration number for that car.	**1**

Answer 14

<table>
<tr>
<td>6(a)</td>
<td>1 mark each to max 5

• The sender hashes the document
• ... to produce a digest
• The sender encrypts the digest to create the digital signature
• The message and the signature are sent to the receiver
• The receiver decrypts the signature to reproduce the digest
• The receiver uses the same hashing algorithm on the document received to produce a second digest
• The receiver compares this digest with the one from the digital signature
• If both of the receiver's digests are the same the document is authentic</td>
<td>5</td>
</tr>
<tr>
<td>6(b)</td>
<td>1 mark each for identification and appropriate description of 2 pieces of software, max 2
<table>
<tr><th>Type of software</th><th>Description</th></tr>
<tr><td>Antivirus</td><td>• scans the computer for viruses and checks against a stored database of viruses, that needs to be updated regularly and then deletes / quarantines them
• compares downloaded files to a database of known viruses and prevents the download continuing</td></tr>
<tr><td>Antispyware</td><td>• scans the computer for spyware and checks against a stored database of viruses, that needs to be updated regularly and then deletes / quarantines them
• compares downloaded files to a database of known spyware and prevents the download continuing.</td></tr>
<tr><td>Firewall</td><td>• monitors incoming and outgoing traffic and compares it to criteria that are set by the user such as through a whitelist/blacklist/identifying allowed / blocked IP addresses
• compares incoming and outgoing traffic to criteria blocks those that do not match criteria</td></tr>
<tr><td>Antimalware</td><td>• scans the computer for viruses and checks against a stored database of viruses, that needs to be updated regularly and then deletes / quarantines them
• compares downloaded files to a database of known viruses and prevents the download continuing</td></tr>
</table>
</td>
<td>2</td>
</tr>
</table>

Answer 15

5(a)	**1 mark** for: Either • Ensuring data can only be accessed by / disclosed to authorised persons Or • Ensuring data cannot be accessed by / disclosed to unauthorised persons	**1**
5(b)	**1 mark** for each bullet point (**max 1**) • Ensuring the accuracy / completeness / consistency of data (during / after processing) • Ensuring the data is up to date	**1**
5(c)	**1 mark** for each bullet point. Phishing email (**max 2**) • The email pretends to be from an official body • ... persuading individuals to disclose private information // by example such as bank details • ... or requesting authentication by redirecting to an unofficial/unauthorised website // inviting a user to click a link Spyware (**max 2**) • Malware downloaded **without the user's knowledge** • ... which secretly records the user's actions / keystrokes on the computer • ... and sends logs of the actions to a third party	**4**

Answer 16

8(a)	**1 mark** for each bullet point (**max 2**) • Validation // a validation method named or described • …protects the data by ensuring that the data is reasonable / sensible and within specified bounds	**2**
8(b)	**1 mark** for difference **1 mark** for similarity Difference: • Pharming is malicious code that redirects to a **fake website**. Phishing uses an **email** to prompt user action. • Pharming is **automatic**. Phishing requires **user action**. Similarity: • Both try to obtain financial or personal information • Both are a false representation of an official organisation, e.g. a bank • Both make use of fake websites	**2**
8(c)	**1 mark** for each bullet point (**max 3**). • Download programs from reputable websites / sources • …as these are less likely to contain malware • Backup / archive computer systems • …so they can be restored in case of data loss from malware program installation • **Install and run** anti-malware program • …so that regular scans can be made for known malware • …and if malware is found it can be quarantined / removed • …and computer's anti-malware definitions are regularly updated • Using a firewall to block unused ports • …so that malware cannot enter the computer system • Deny administrator privileges to everyday users • …so that malware cannot be downloaded by everyday users • Avoid the use of / access to removable devices • …so that malware cannot be installed from these devices	**3**

Answer 17

5(b)	**1 mark** for each correctly completed term: • odd or even • 7-bits • odd • block • byte Computer A and Computer B agree on whether to use **odd or even** parity. Computer A divides the data into groups of **7-bits**. The number of 1s in each group is counted. If the agreed parity is **odd** and the group has an even number of 1s a parity bit of 1 is appended, otherwise a parity bit of 0 is appended. In a parity **block** check the bytes are grouped together, for example in a grid. The number of 1s in each column (bit position) is counted. A bit is assigned to each column to make the column match the parity. These parity bits are transmitted with the data as a parity **byte**.	**5**
5(c)(i)	**1 mark** each to **max 3**: • Compares all incoming and outgoing transmissions • ... against set criteria/whitelist/blacklist • Blocks all transmissions that do not meet rules • Blocks data entering from specific ports • Blocks unauthorised/unknown internal software transmitting data	**3**

Answer 18

3(a)(i)	**1 mark** for security measure **1 mark** each to **max 2** for how the chosen measure works: • Firewall • Checks **incoming** connections • ... against criteria • Blocks data from entering specific ports • Blocks data that does not meet whitelist that meets blacklist • Proxy server • Prevents devices accessing the web server directly • Intercepts any requests • Forwards the request using its own IP address • Screens returning data before sending it to the user	**3**
3(a)(ii)	**1 mark** for security measure **1 mark** each to **max 2** for description of the chosen measure: • Encryption • Encodes/scrambles data • ... so if it is intercepted it cannot be **understood** • Algorithm/key is required to decode the data	**3**

Answer 19

<table>
<tr>
<td>7(f)(i)</td>
<td>1 mark for each correct method and
1 mark for corresponding description to max 4:

<table>
<tr><th>Method</th><th>Description</th></tr>
<tr><td>Parity byte</td><td>An additional bit is added to make the number of 1s in the byte odd or even to match the parity. If a byte with an odd number of 1 bits is received when even parity is used, there is an error.</td></tr>
<tr><td>Parity block</td><td>Parity is calculated horizontally and vertically. A parity byte is created from the bits produced by the vertical parity check. This is sent with the data. The parity is re-checked when received and the position of an incorrect bit can be determined.</td></tr>
<tr><td>Checksum</td><td>A calculation is made from the data and the result transmitted with the data. The receiver repeats the calculation and compares the result with the value received. If the two are different, there is an error.</td></tr>
</table>
</td>
<td>4</td>
</tr>
<tr>
<td>7(f)(ii)</td>
<td>1 mark each to max 2:

• Encodes/scrambles data
• ... so if it is intercepted it cannot be understood
• Algorithm/key is required to decode the data</td>
<td>2</td>
</tr>
</table>

Answer 20

<table>
<tr><th>Question</th><th>Answer</th><th>Marks</th></tr>
<tr><td>1(a)</td><td>1 mark for each correctly completed term.

Validation checks that the data entered is reasonable. One example is a presence check.
Verification checks that the data entered is the same as the original. One example is double entry.</td><td>4</td></tr>
<tr><td>1(b)</td><td>1 mark for each correct entry

<table>
<tr><th>Security measure</th><th>Description</th></tr>
<tr><td>Disk mirroring</td><td>Data are written on two or more disks simultaneously.</td></tr>
<tr><td>Encryption</td><td>Contents are scrambled so they cannot be understood without a decryption key</td></tr>
<tr><td>Backup</td><td>A copy of the data is taken and stored in another location</td></tr>
</table>
</td><td>3</td></tr>
</table>

Answer 21

<table>
<tr><td>7(d)(i)</td><td>1 mark per bullet point to max 2

• Prevents unauthorised access to the data
• Monitors incoming and outgoing traffic
• Blocks transmissions from unauthorised sources / websites / ports
• Maintains an allow list / deny list of IP addresses</td><td>2</td></tr>
</table>

<table>
<tr><th>Question</th><th>Answer</th><th>Marks</th></tr>
<tr><td>7(d)(ii)</td><td>1 mark only from:

• Running up-to-date antivirus software
• Use of proxy server
• Strong / Biometric passwords
• Etc.</td><td>1</td></tr>
</table>

Answer 22

5(a)	**1 mark** per bullet point to **max 3** • Encryption scrambles the source code (so it is meaningless) • … using an encryption key / algorithm • If the file is accessed without authorisation it will be meaningless • It requires a decryption key / algorithm to unscramble	3

Answer 23

4(b)	**1 mark** per bullet point to **max 2 · 2** Data backup ▯ A copy of data will have been made and stored elsewhere. ▯ If the original is lost, the backup can be used to restore the data. Disk-mirroring ▯ The data is stored on two disks simultaneously. ▯ If the first disk drive fails, the data is accessed from the second disk.	4

Answer 24

2(a)	**1 mark** per bullet point • Security: keep data safe from accidental/malicious damage/loss • Privacy: keep data confidential // only seen by authorised personnel	**2**
2(b)	**1 mark** for identifying method **2 marks** for description to **max 2 × 3** For example: • User accounts • User has a username and password Access to resources can be limited to specific accounts • Cannot access system without valid username and password // prevents unauthorised access to the system • Firewall • All incoming and outgoing network traffic goes through firewall • Blocks signals that do not meet requirements • Keeps a log of signals • Applications can have network access restricted • Anti-malware • Scans for malicious software • Quarantines or deletes any malicious software found • Scans can be scheduled at regular intervals • Should be kept up to date • Auditing • Logging all actions/changes to the system • In order to identify any unauthorised use • Application Security (accept equivalent) • Applying regular updates / patches • Finding, fixing and preventing security vulnerabilities in any (installed) application	**6**
2(c)(i)	**1 mark** per bullet to **max 4** • Each byte has a parity bit // horizontal parity • An additional parity byte is sent with vertical (and horizontal) parity • Each row and column must have an even/odd number of 1s • Identify the incorrect row and column • The intersection is the error	**4**
2(c)(ii)	**1 mark** for correct answer • Errors in an even number of bits (could cancel each other out)	**1**

Answer 25

1(c)(ii)	**1 mark** for each security method to **max 2**, **1 mark** for integrity **Security** - encryption - access rights - username and password // biometrics // user accounts - backup // disk mirroring - firewall - Physical methods (e.g. CCTV, locked rooms etc.) **Integrity** - checksum - parity - validation on input	3

Answer 26

<table>
<tr>
<td>6(b)(i)</td>
<td>1 mark for the correct bit circled
<table>
<tr><td></td><td>Parity bit</td><td colspan="7">Data</td></tr>
<tr><td></td><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td></td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td></tr>
<tr><td></td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td><td>1</td><td>1</td></tr>
<tr><td></td><td>1</td><td>1</td><td>1</td><td>0</td><td>1</td><td>(1)</td><td>1</td><td>1</td></tr>
<tr><td>Parity byte</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td></tr>
</table>
</td>
<td>1</td>
</tr>
<tr>
<td>6(b)(ii)</td>
<td>1 mark for each bullet point
▯ row and column has incorrect parity (odd instead of even)
▯ the intersection identifies the error</td>
<td>2</td>
</tr>
<tr>
<td>6(c)</td>
<td>1 mark per bullet to max 2
▯ Errors in an even number of bits (in the same row or column)
▯ Prevents error being identified
▯ Could appear to be correct</td>
<td>2</td>
</tr>
<tr>
<td>6(d)</td>
<td>1 mark for the name and max 2 marks for description
▯ Check sum
▯ A calculation is done on a block of data
▯ The result is transmitted with the data
▯ Calculation repeated at receiving end
▯ Results compared
▯ If different an error has occurred

▯ Hash total
▯ Total of several fields of data
▯ Including fields not usually used in calculations
▯ The result is transmitted with the data
▯ Calculation repeated at receiving end
▯ Results compared
▯ If different an error has occurred</td>
<td>3</td>
</tr>
</table>

Answer 27

<table>
<tr><th>Question</th><th>Answer</th><th>Marks</th></tr>
<tr><td>3(a)</td><td>1 mark for correct parity bit

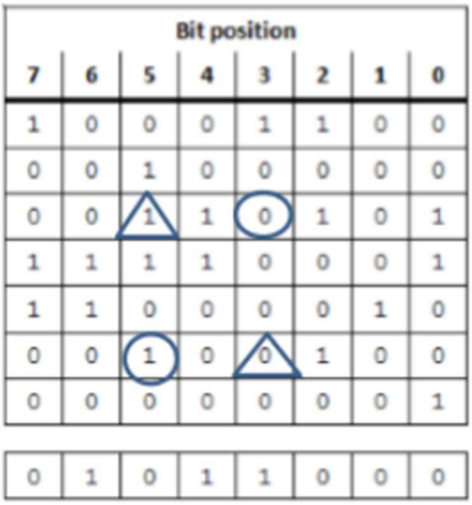
Parity bit
<table><tr><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr></table></td><td>1</td></tr>
<tr><td>3(b)</td><td>1 mark for the correct bit circled.
<table><tr><th>Parity bit</th><th colspan="7">Data</th></tr><tr><td>1</td><td>0</td><td>1</td><td>0</td><td>1</td><td>1</td><td>1</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td></tr><tr><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>Parity byte</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td></tr></table></td><td>1</td></tr>
<tr><td>3(c)</td><td>1 mark per each correct row

<table><tr><th>Measure</th><th>Validation</th><th>Verification</th></tr><tr><td>Checksum</td><td></td><td>✓</td></tr><tr><td>Format check</td><td>✓</td><td></td></tr><tr><td>Range check</td><td>✓</td><td></td></tr><tr><td>Double entry</td><td></td><td>✓</td></tr><tr><td>Check digit</td><td>✓</td><td></td></tr></table></td><td>5</td></tr>
</table>

Answer 28

4(a)	**Parity bit** **1** 0 1 1 1 0 1 0	**1**
4(b)	**1 mark** for correctly circled bit **Parity bit** | **Data** **0** 0 1 1 0 1 0 1 **1** 1 1 1 1 0 0 1 **1** 0 1 0 1 0 **(0)** 0 **0** 0 0 1 1 0 1 1 **Parity byte** **0** **1** **1** **1** **1** **1** **0** **1**	**1**
4(c)	**1 mark** for each correct line **Error detection measure** Type check → Validation Proof reading → Verification Check digit → Validation Checksum → Verification	**4**

Answer 29

5(a)(i)	□ Count the number of one bits in the <u>first seven</u> bit positions 1 □ Add a 0 or 1 to bit position 0, to make the count of one bits an <u>odd</u> number 1	**2**
5(a)(ii)	A = 1 B = 1	**1**
5(a)(iii)	**<u>Two</u>** from: □ A parity bit is worked out for each <u>column</u> 1 □ The computer checks the parity of each bit position in parity byte // the computer generates copy of the parity byte and <u>compares</u> 1 □ If incorrect parity then there is an error in the data received // No parity error means no error in the data received 1 □ The position of the incorrect bit can be determined 1	**2**
5(b)(i)		**2**
5(b)(ii)	**<u>Three</u>** from: □ Consider each row in sequence 1 □ Identify any row with incorrect parity 1 □ Repeat the process for each column in sequence 1 □ Identify where a row and column with incorrect parity intersect 1	**3**

Answer 30

<table>
<tr><td>3(a)</td><td>Two marks from:

▯ Physical measures
▯ Access rights
▯ Encryption
▯ Firewall
▯ Use authentication methods such as usernames and passwords
▯ Anti-malware program</td><td>Max 2</td></tr>
<tr><td>3(b)(i)</td><td>
<table>
<tr><td>7</td><td>X</td><td>6</td><td>=</td><td>42</td></tr>
<tr><td>8</td><td>X</td><td>5</td><td>=</td><td>40</td></tr>
<tr><td>6</td><td>X</td><td>4</td><td>=</td><td>24</td></tr>
<tr><td>5</td><td>X</td><td>3</td><td>=</td><td>15</td></tr>
<tr><td>3</td><td>X</td><td>2</td><td>=</td><td>6</td></tr>
<tr><td>1</td><td>X</td><td>1</td><td>=</td><td>1</td></tr>
<tr><td></td><td></td><td></td><td>Total:</td><td>128 / 11</td></tr>
<tr><td></td><td></td><td></td><td></td><td>11 R 7</td></tr>
<tr><td colspan="4">Check digit:</td><td>11 – 7 = 4</td></tr>
</table>
1 mark for 6 values
1 mark for 2 steps
Accept 128 MOD 11 = 7
1 mark for subtraction

Answer: 786531 4 (1 mark for answer)</td><td>4</td></tr>
<tr><td>3(b)(ii)</td><td>One mark for name of check
One mark for description
Max two checks

Uniqueness check
Each <code>PatientID</code> must be unique

Length check
Each <code>PatientID</code> is exactly 7 characters

Format check / Type check
All 7 characters must be digits

Presence check
<code>PatientID</code> must be entered</td><td>Max 4</td></tr>
</table>

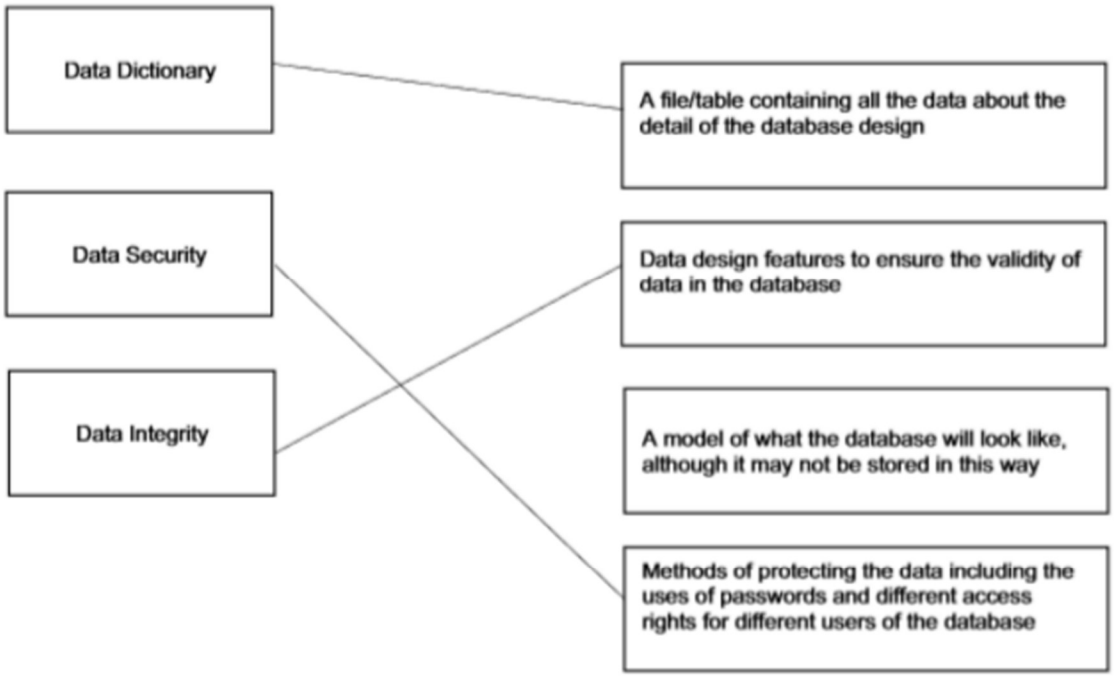
Answer 31

3(a)(i)	**1 Mark** per bullet, max 3 ▯ Security is keeping the data safe ▯ From accidental / malicious damage /loss ▯ By example of need for security ▯ Privacy is the need to restrict access to personal data ▯ To avoid it being seen by unauthorised people ▯ By example of need for privacy	**3**
3(a)(ii)	**1 Mark** for a suitable example For example: Personal data of students / staff	**1**

3(a)(ii)	**1 Mark** for a suitable example For example: Personal data of students / staff	**1**
3(b)	**1 Mark** for stating the security measure **1 Mark** for a corresponding description Maximum 2 marks for each measure Maximum 2 measures **Physical measures** - Locked doors/keyboards etc. - Secure methods of access, keypads/ biometric scans etc. **Backup of data** - Regular copies of the data are made - If the data is corrupted it can be restored **Disk-mirroring** - All activity is duplicated to a second disk in real time so that if the first disk fails there is a complete copy available **Access rights** - Different access rights for individuals/groups of users - To stop users editing data they are not permitted to access - By example **Encryption** - If accessed, data cannot be understood by unauthorised personnel - Accessed only by those with the decryption key **Firewall** - To stop unauthorised access/hackers gaining access to the computer network **Use authentication methods such as passwords and usernames** - Passwords should be strong / biometrics - To prevent unauthorised access to data **Anti-malware program** - To detect / remove / quarantine viruses / key-loggers etc. - Carrying out regular scans **Concurrent Access Controls // Record locking** - Closes a record to second user until first update complete - To prevent simultaneous updates being lost	**4**

3(c)	**1 Mark** per bullet, max 2 - Checking that the data entered matches / is consistent with that of the source. - Comparison of two versions of the data - Examples include double entry, visual checking, proof reading etc... - In the event of a mismatch – the user is forced to re-enter the data - By example, e.g. creation of a password - Does not check data is sensible/acceptable	**2**

Answer 32



(b) **One mark** for procedure point, **one mark** for justification. **[6]**

Maximum **three** procedures.

- How often should the data be backed up? e.g. at the end of each day
- Justification e.g. student's progress may be edited each day and should not be lost

- What medium should the data be backed up to? e.g. external hard disk drive
- Justification e.g. it has large enough capacity

- Where should the backups be stored? e.g. off-site
- Justification e.g. so if the building is damaged only the original data are lost

- What is backed up? e.g. only updated files ...
- Justification e.g. There are a large number of files and they are not all updated each day

- When should the backup take place? e.g. overnight
- Justification e.g. the system is not likely to be used then

- Who is responsible for performing the backup?
- Justification e.g. otherwise it may not be done

- Make sure the procedure is written down and understood by staff
- Justification e.g. otherwise some data may not be backed up

Answer 33

(a) Four from: **[4]**

- Security is keeping the data safe.
- Integrity is making sure that the data is correct / valid.
- Security is the prevention of data loss.
- Integrity ensures that the data received is the same as the data sent / data copied is the same as the original.
- Example of ensuring security, e.g. usernames and passwords, firewalls etc...
- Example of ensuring integrity, e.g. parity checks, double entry etc...

(b) Three pairs from: **[6]**

- Installing a firewall and ensuring it is switched on.
- To stop unauthorised access / hackers gaining access to the bank's computer network.

- Use authentication methods such as passwords and usernames.
- Passwords should be strong / biometrics.

- Encrypt the data.
- So that if data is accessed it will be meaningless / only accessed by those with decryption key.

- Set up access rights...
- To stop users reading/editing data they are not permitted to access.

- Installing and running an up to date anti-malware program (anti-virus/anti-spyware etc.).
- To detect / remove / quarantine viruses / key-loggers etc.

- Make regular backups of the data.
- To separate device or off site to enable recovery if necessary.

- Employ measures for physical security.
- Example of a measure for physical security.

Answer 34

(c) (i)
- Hackers can still access the data (and corrupt it, change it or delete it)
- Encryption simply makes data incomprehensible (without decryption key / algorithm)

[2]

(ii) Any **two** from:

- This is an explanation of data verification (not validation)
- Data validation ensures that data is reasonable / sensible / within a given criteria
- Original data may have been entered correctly but is not reasonable (e.g. age of 210)

[2]

(iii)
- A password does not prevent unauthorised access, it makes it more difficult
- Password can be guessed (if weak) // Password can be stolen // A relevant example of misappropriation of password

[2]

Answer 35

(a) maximum of **two marks** for firewall description + maximum of **two marks** for authe description

Firewall

- sits between the computer or LAN and the Internet/WAN and permits or blocks traffic to/from the network
- can be software and/or hardware
- software firewall can make precise decisions about what to allow or block as it can detect illegal attempts by specific software to connect to Internet
- can help to block hacking or viruses reaching a computer

Authentication

- process of determining whether somebody/something is who/what they claim to be
- frequently done through log on passwords/biometrics
- because passwords can be stolen/cracked, digital certification is used
- helps to prevent unauthorised access to data [3]

(b) **one** mark for security, **one** mark for integrity:

- integrity deals with validity of data/freedom from errors/data is reasonable
- security deals with protection of data
- security protects data from illegal access/loss
- integrity deals with making sure data is not corrupted after, for example, being transmitted [2]

(c) **(i)** **one mark** for each way of maintaining data security + **one mark** for an example/ enhancement

- validation (to ensure data is reasonable)
- examples include range checks, type checks, length checks, …

- verification (checks if data input matches original/if transmitted data matches original)
- can use double data entry or visual check/other methods such as parity checks
- doesn't check whether or not data is reasonable [3]

(ii) **one mark** for each way of maintaining data integrity + **one mark** for an example/ enhancement

- parity checking
- one of the bits is reserved as parity bit
- e.g. 1 0 1 1 0 1 1 0 uses odd parity
- number of 1s must be odd
- parity is checked at receiver's end
- a change in parity indicates data corruption

- check sum
- adds up bytes in data being sent and sends check sum with the data
- calculation is re-done at receiver's end
- if not the same sum then the data has been corrupted during transmission [3]

Answer 36

(a) One mark for validation, one mark for verification.

validation

– check whether data is reasonable / meets given criteria

verification

– method to ensure data which is copied / transferred is the same as the original
– entering data twice and computer checks both sets of data
– check entered data against original document / source [2]

(b) any **four** from:

– parity can be even or odd
– parity check uses the number of 1s in a binary pattern
– if there is an even / odd number of 1s, then the parity is even / odd
– following transmission …
– parity of each byte checked
– a parity bit is used to make sure binary pattern has correct parity
– example: 1 0 0 1 0 1 1 1 has parity bit set to 1 in MSB since system uses odd parity (original data: 0 0 1 0 1 1 1 which has four 1 bits) [4]

Answer 37

(a) any **two** from:

- malicious code / software / program
- that replicates / copies itself
- can cause loss of data / corruption of data on the computer
- can cause computer to "crash" / run slowly
- can fill up hard disk with data [2]

(b) any **two** from:

- checks for boot sector viruses when machine is first turned on
- when an external storage device is connected
- checks a file / web page when it is accessed / downloaded [2]

Answer 38

(Not Available)

Answer 39

(a) Data transmitted in both directions BUT only 1 direction at a time [1]

(b) **(i)** **1** 1 0 1 0 0 0 1 [1]

(ii) Any **two** points from:

- computer "B" counts number of 1-bits
- if number of 1-bits is even then byte has been transmitted correctly
- if number of 1-bits is odd then byte has been corrupted during transmission [2]

(c) 1 0 1 1 0 1 1 1

0 1 1 1 1 0 0 0

⟶ 0 0 0 1 **1** 0 1 0

0 1 1 1 0 0 0 1
- - - - - - - - - - -
1 0 1 0 1 1 0 0
- - - - - - - - - - -

(i) (see diagram above). 1 mark for identifying third byte and 1 mark for identifying 5th bit as an error [2]

(ii) corrected byte

0	**0**	**0**	**1**	**0**	**0**	**1**	**0**

[1]

(iii) Any **two** from:

- for example, a check sum
- brief description of check sum
- description of alternative checking method
- ask for data to be re-sent [2]

Answer 40

(a) – a program that can self-replicate
can delete or corrupt data from a computer system
malicious code often installed without the user's knowledge **[1]**

(b) Any **three** from:

- install **and** run/use anti-virus software
- update anti-virus software on a regular basis
- avoid programs/software/downloads from unknown sources
- never "double click" on email attachments which are executable i.e. contain .exe, .com or .vbs
- install and run/use a firewall (which screens incoming Internet and network traffic)
- install and run/use anti-spyware software (which works in conjunction with the anti-virus to stop viruses doing any harm to the computer)
- avoid suspicious web sites
- delete emails from unknown contacts without opening
- avoid using media from unknown sources **[3]**

Answer 41

(b) (i)

letter	bytes adjusted for even parity							
C	1	*1*	*0*	*0*	*0*	*0*	*1*	*1*
O	1	*1*	*0*	*0*	*1*	*1*	*1*	*1*
M	0	*1*	*0*	*0*	*1*	*1*	*0*	*1*
P	0	*1*	*0*	*1*	*0*	*0*	*0*	*0*
U	0	*1*	*0*	*1*	*0*	*1*	*0*	*1*
T	1	*1*	*0*	*1*	*1*	*0*	*0*	*0*
I	1	*1*	*0*	*0*	*1*	*0*	*0*	*1*
N	0	*1*	*0*	*0*	*1*	*1*	*1*	*0*
G	0	*1*	*0*	*0*	*0*	*1*	*1*	*1*

(–1 mark for each error in the first column) [2]

(ii) 0 1 0 1 1 1 0 0 [1]

(iii) Any **three** points from:

character "P" flagged as having *odd parity* (row 4 in diagram)
parity byte sent with data i.e. 0 1 0 1 1 1 0 0
column 5 also has *odd parity* (or equivalent)
faulty bit must be in row 4 and column 5
idea of auto correction of fault (in row 4, column 5)

(Check if diagram has been annotated to show faulty bit) [3]

Answer 42

(a) (i) character "A" [1]

(ii) column number: 6
row number: 8 [1]

(iii) Any **three** points from:

character "A" is showing *even parity*
column 6 is also showing *even parity*
where the column and row intersect is position (6, 8)
the bit value here should be 0 and not 1 [3]

(b) Any **three** points from:

bytes sent as a block
bytes added up before transmission
result of addition is sent with the data block
same calculation is carried out at receivers end
the two values are compared [3]