Data Transmission

(Chapter 2)

Syllabus Content:

2.1 Types and methods of data transmission

Candidates should be able to:	Notes and guidance
1 (a) Understand that data is broken down into packets to be transmitted	
(b) Describe the structure of a packet	• A packet of data in a unit of data contains a – packet header – payload – trailer • The packet header includes the: – destination address – packet number – originator's address
(c) Describe the process of packet switching	• Data is broken down into packets • Each packet could take a different route • A router controls the route a packet takes • Packets may arrive out of order • Once the last packet has arrived, packets are reordered
2 (a) Describe how data is transmitted from one device to another using different methods of data transmission	• Including: – serial – parallel – simplex – half-duplex – full-duplex
(b) Explain the suitability of each method of data transmission, for a given scenario	• Including the advantages and disadvantages of each method
3 Understand the universal serial bus (USB) interface and explain how it is used to transmit data	• Including the benefits and drawbacks of the interface

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

Syllabus Content:

2.2 Methods of error detection

Candidates should be able to:	Notes and guidance
1 Understand the need to check for errors after data transmission and how these errors can occur	• Errors can occur during data transmission due to interference, e.g. data loss, data gain and data change
2 Describe the processes involved in each of the following error detection methods for detecting errors in data after transmission: parity check (odd and even), checksum and echo check	• Including parity byte and parity block check
3 Describe how a check digit is used to detect errors in data entry and identify examples of when a check digit is used, including international standard book numbers (ISBN) and bar codes	
4 Describe how an automatic repeat query (ARQ) can be used to establish that data is received without error	• Including the use of: – positive/negative acknowledgements – timeout

2.3 Encryption

Candidates should be able to:	Notes and guidance
1 Understand the need for and purpose of encryption when transmitting data	
2 Understand how data is encrypted using symmetric and asymmetric encryption	• Asymmetric encryption includes the use of public and private keys

2 Data Transmission

2.1 | Types & Methods of Data Transmission

NOTE: Data Packets & Packet Switching are newly added topics in the Computer Science (2210) syllabus for the session 2023–2025.

2.1.1 Data Packets:

- The data is broken down into packets to be transmitted.
- The packets of data are usually quite small, typically 64 KiB.

Packet Structure:

- A packet of data in a unit of data has a packet header.
- The header contains the destination address, packet number & the originator's address.
- The packet also has a payload and a trailer.

<table>
<tr><th>Header</th><th>Payload</th><th>Trailer</th></tr>
<tr><td>It consists of the IP address of the sender</td><td rowspan="4">It consists of the actual data being sent in the packet (usually about 64 KiB)</td><td rowspan="2">It consists of some way of identifying the end of the packet which is essential for packet separation after transmission</td></tr>
<tr><td>It consists of IP address of the receiver/destination.</td></tr>
<tr><td>It consists of the sequence number of the packet which allows correct reassembly after transmission</td><td rowspan="2">It consists of an error checking method called cyclic redundancy checks (CRCs) to ensure packet arrives error-free</td></tr>
<tr><td>It consists of the size of packet (in bytes)</td></tr>
</table>

Purpose of Packet Header:

- It stores data about the packet and its routing to ensure it reaches its destination.
- It ensures that the message can be properly reconstructed.

Cyclic Redundancy Checks (CRCs):

- It is an error checking method used to check data packets.
- It involves the sending computer adding up all the 1-bits in the payload and storing this as a hex value in the trailer before transmission.
- After transmission, the receiving computer recalculates the number of 1-bits in payload.
- The two values are compared and if they match then no transmission errors occur.
- If they do not match, then the packet needs to be re-sent.

Packet Switching:

- The data is broken down into packets.
- Each packet is given its own route.
- The routing for a packet depends on the congestion.
- The packets may not arrive in the order sent.

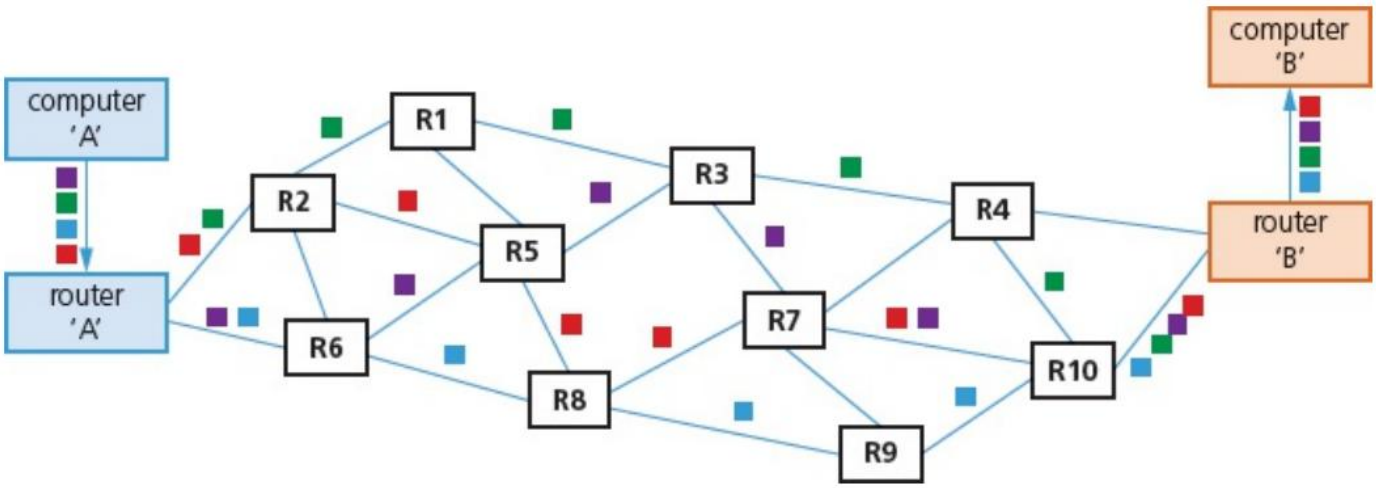
Process of Packet Switching:

- A large message is broken down into a group of smaller chunks of the same size called packets.
- Each packet is dispatched independently and may travel along different routes/paths.
- A router controls the route taken by a packet and decides where to send packet next for the most efficient path.
- The packets may arrive out of order and are reassembled into the original message at the destination (using the information sent in the packet header).
- If packets are missing/corrupted, a re-transmission request is sent.

Function of a Router in Packet Switching:

- The router examines the packet's header.
- It reads the IP address of the destination from the packet header.
- A router has access to a routing table which contains information about, e.g., available hops/netmask/gateway used and the status of the routes along the route.
- The router decides on the next hop/best route and sends the packet on its next hop.

Diagram of Packet Switching:



- The message sent by computer 'A' was split into four packets.
- The original packet order was: ■■■■
- They arrived in the order: ■■■■
- It means they need to be reassembled in the correct order at the destination.

Advantages of Packet Switching:

1. It makes best use of the available (channel) capacity by using alternative routes.
2. It ensures accurate delivery of the message.
3. The use of alternative routes is more secure as harder to intercept messages.
4. It provides better security as packets are hashed and sent by different routes.
5. The use of alternative routes is more robust, and path/route is also available to other users.
6. The missing packets can be easily detected and a re-sent request is sent so the message arrives complete.
7. If a network changes, the router can detect this and send the data another way to ensure it arrives.
8. It doesn't use whole/complete bandwidth.
9. It allows simultaneous use of channels by multiple users.

Disadvantages of Packet Switching:

1. There are time delays to reassemble packets at the destination and correcting errors.
2. The packets can be lost and need to be re-sent.
3. The network problems may introduce errors in packets.
4. It requires complex protocols for delivery.
5. It is unsuitable for real-time transmission applications/real-time streaming e.g. a live sporting event being transmitted over the internet.

Uses of Packet Switching:

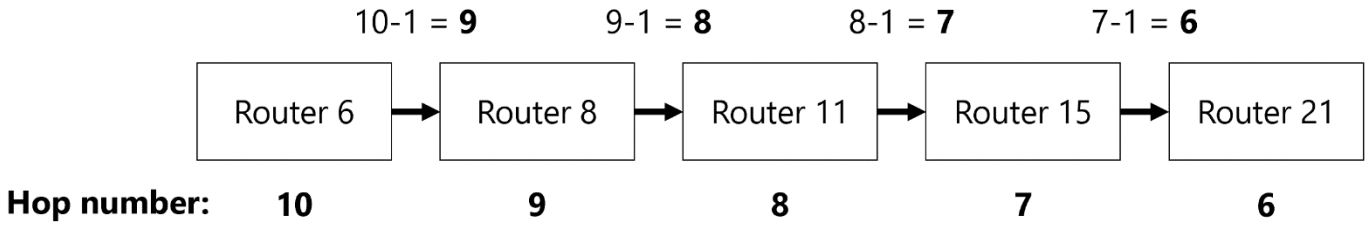
1. It is used in sending email messages.
2. It is used in Voice over Internet Protocol (VoIP).
   It is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line.

Hopping:

- Sometimes it is possible for packets to get lost and keep 'bouncing' around from router to router and never actually get to their destination.
- Eventually, the network could grind to a halt as the number of 'lost' packets mounts up and clogs up the system.
- To overcome this, a method called hopping is used.

Process of Hopping:

- A hop number is added to the header of each packet.
- Each packet is only allowed to hop a limited number of times (this number is determined by the network protocol and routing table being used).
- Each time a packet passes through a different router, the hop number is decreased by 1 as shown below:



- If the packet has not reached its destination and the hop number becomes 0, then the packet will be deleted when it reaches the next router.
- The missing packets will then be flagged by the receiving computer and the request to re-send these packets will be made.

Exam Style Questions:

Question 1:

A company has a website that is stored on a web server.

(a) The website data is broken down into packets to be transmitted to a user.

Describe the structure of a data packet.

.....

.....

.....

.....

.....

.....

.....

..... [4]

Answer:

Question	Answer	Marks
2(a)	Any **four** from: • it has a header • … that contains the destination address • … that contains the packet number • … that contains the originator's address • it has a payload • it has a trailer.	4

Question 2:

(b) (i) Describe packet switching.

.....

.....

.....

.....

.....

..... [3]

Answer:

3(b)(i)	Any **three** from: • A circuit does not have to be established at the start of the communication • The data to be sent is divided into packets • That can travel along different routes • From node to node • Packets are reassembled in the correct order at the receiver's end • Must wait until the last packet is received to put the data back together	**3**

Question 3:

Give **two** benefits **and two** drawbacks of packet switching.

Benefit 1 .....

.....

Benefit 2 .....

.....

Drawback 1 .....

.....

Drawback 2 .....

.....

[4]

Answer:

Question	Answer	Marks
6	**One** mark for each correct benefit **(Max 2)** • Accuracy – Ensures accurate delivery of the message • Completeness – Missing packets can be easily detected and a re-send request sent so the message arrives complete • Resilience – if a network changes the router can detect this and send the data another way to ensure it arrives • Path also available to other users // Doesn't use whole bandwidth // allows simultaneous use of channel by multiple users • Better security as packets hashed and sent by different routes. **One** mark for each correct drawback **(Max 2)** • Time delays to correct errors // Network problems may introduce errors in packets • Requires complex protocols for delivery • Unsuitable for real time transmission applications	**4**

Question 4:

(a) Explain how packet switching is used to transfer messages across the internet.

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [5]

(b) Outline the function of a router in packet switching.

.....

.....

.....

.....

.....

.....

..... [3]

Answer:

Question	Answer	Marks
6(a)	**One** mark for each correct marking point **(Max 5)** • A large message is divided up into a group of smaller chunks of the same size called **packets** • The packet has a header and a payload • The header contains a source **IP** address, destination **IP** address (and sequence number) • Each packet is dispatched independently • … and may travel along different routes / paths • The packets may arrive out of order • … and are reassembled into the original message at the destination • If packets are missing / corrupted a re-transmission request is sent.	**5**
6(b)	**One** mark for each correct marking point **(Max 3)** • The router examines the packet's header • It reads the IP address of the destination (from the packet header) • A router has access to a routing table • …containing information about, e.g., available hops / netmask / gateway used • … and the status of the routes along the route • … the router decides on the next hop / best route • … and sends the packet on its next hop.	**3**

2.1.2 Data Transmission:

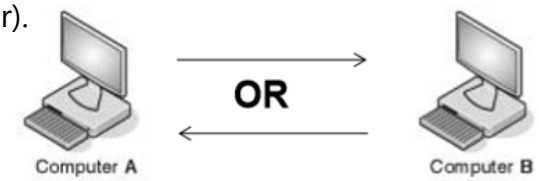
According to our syllabus, we will consider three factors regarding data transmission:

1. The **direction** of data transmission.
2. The **method of transmission**.
3. The **method of synchronization** between the two devices.

Direction of Data Transmission:

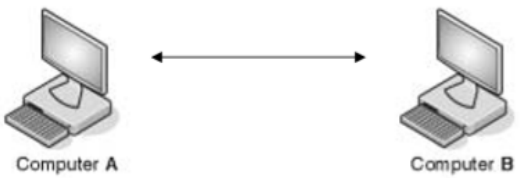
1) Simplex Data Transmission:

- It is in **one direction** only (i.e. from sender to receiver).
- **Example**: data sent from computer to a printer, microphone to computer, sensor to computer, computer to speaker, computer to monitor etc.



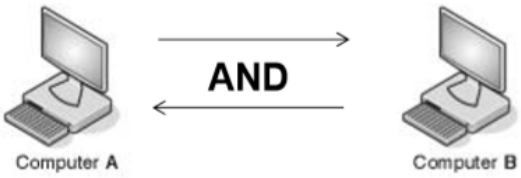
2) Half-duplex Data Transmission:

- It is in **both directions** but **not at the same time**.
- **Example**: a phone conversation between two people where only one person speaks at a time, a video conference where only one person speaks at a time etc.



3) Full-duplex Data Transmission:

- It is also called "Duplex data transmission".
- It is in **both directions simultaneously** (at the same time).
- **Example**: broadband connection on a phone line, instant messaging, computer to modem etc.

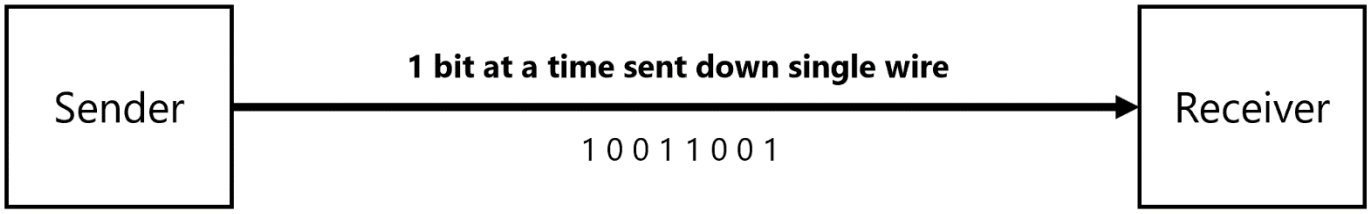


Methods of Data Transmission:

It means bits are sent one after the other in a single stream.

1) Serial Data Transmission:

- It is when data is sent, one bit at a time, over a single wire or channel.
- The bits arrive in sequence.
- It can be synchronous or asynchronous.



NOTE: Serial data transmission can be simplex, half-duplex or full-duplex.

Advantages of Serial Transmission:

It uses a single wire/channel hence:

1. It is more reliable over longer distances.
2. The cost of wiring is less expensive since a single wire is used.
3. Single wire means less chance of interference/data corruption.

Data is sent one bit at a time so:

4. The data is sent more accurately over longer distances.
5. There is less chance of data being skewed.

Disadvantages of Serial Transmission:

It uses a single wire/channel hence:

1. Data is transmitted at a slower rate.

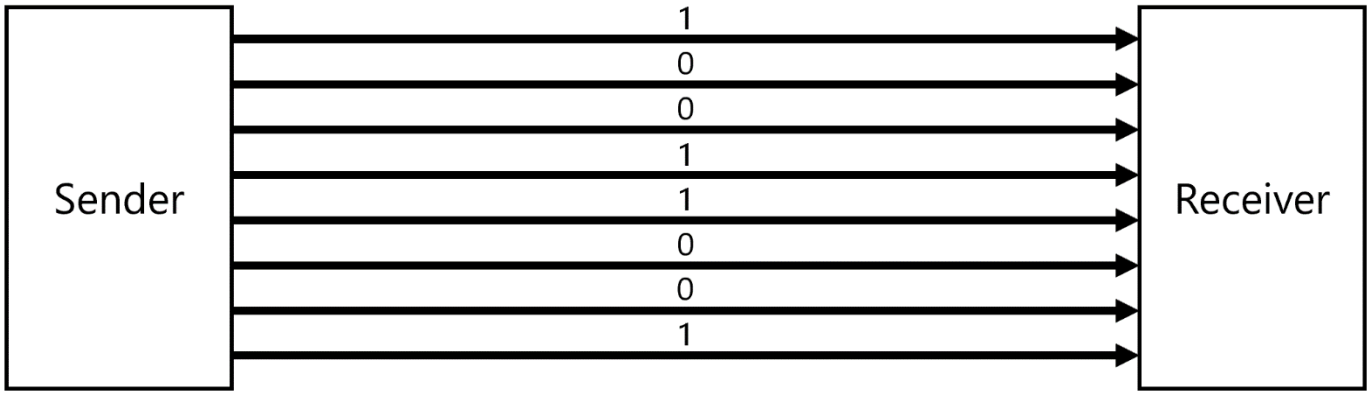
Applications of Serial Transmission:

1. Sending data from computer to a modem.
2. Data transmission in Universal Serial Bus (USB).
3. Data transmission in Wi-Fi.
4. It is used in places where data transmission is to be done over long distances e.g. 100 meters and above.

2) Parallel Data Transmission:

- It is when several bits of data (usually 1 byte) are sent down several wires or channels at the same time. (one wire or channel is used to transmit each bit)
- The bits may arrive out of sequence.
- It can only be synchronous.

8 bits at a time sent down 8 wire/channels



NOTE: Parallel data transmission can be simplex, half-duplex or full-duplex.

Advantages of Parallel Transmission:

It uses multiple wires/channels hence:

1. Data is transmitted at a faster rate.

Disadvantages of Parallel Transmission:

It uses multiple wires/channels hence:

1. It is less reliable over longer distances.
2. The cost of wiring is more expensive since many wires are used.
3. Multiple wires means more chances of interference/data corruption.

Data is sent several bits at a time:

4. Data is sent less accurately over longer distances.
5. There is a likely chance of data being skewed.

Applications of Parallel Transmission:

1. Sending data from a computer to a printer.
2. Data transmission in internal electronics of computer.
3. Data transmission on pathways between CPU and the memory.
4. Data transmission in integrated circuits (IC), buses and other internal components.
5. It is used in places where data transmission is to be done over shorter distances e.g. 10 metres and less.

Method of Synchronization:

1) Asynchronous Data Transmission:

- It refers to data being transmitted in an agreed bit pattern.
- Data bits (1s and 0s) are grouped together and sent with control bits (without these, it would be impossible to separate groups of data as they arrive).

Advantages of Asynchronous Transmission:

1. It prevents data being mixed up/skewed.

Disadvantages of Asynchronous Transmission:

1. It is a slower method of data transfer.

2) Synchronous Data Transmission:

- It is a continuous stream of data.
- Data is accompanied by timing signals generated by an internal clock (to ensure both sender and receiver are synchronized with each other).
- The receiver counts how many bits (1s and 0s) were sent and then reassembles them into bytes of data.

Advantages of Synchronous Transmission:

1. It is a faster method of data transfer (mostly used in network communications).

Disadvantages of Synchronous Transmission:

1. The timing must be very accurate as there are no control bits sent along otherwise data will be mixed up/skewed.

Exam Style Questions:

Exam Tip:

If examiner tells you that a person is using any of the following be it:

1) serial simplex data transmission
2) serial half-duplex data transmission
3) serial duplex data transmission
4) parallel simplex data transmission
5) parallel half-duplex data transmission
6) parallel duplex data transmission

And asks you to explain why the person is using that specific data transmission method. Just remember that you have to address both parts of the questions to gain full marks. This kind of question is mostly asked for 4 marks and above.

- One part will address the advantages/benefits/choice of using either serial or parallel transmission.
- The other part will address the advantages/benefits/choice of using either simplex, half-duplex or duplex transmission.

If it is a 4 mark question, then 2 statements for direction of transmission + 2 statements for method of transmission will earn you 4 marks.

If you only address either direction or method and forget the other, no more than 2/4 marks can be secured.

Question 1:

A computer includes an Integrated Circuit (IC) and a Universal Serial Bus (USB) for data transmission. Describe how the computer uses these for data transmission, including the type of data transmission used. (4)

- Integrated circuit (IC) is used for sending data internally.
- In IC, parallel data transmission is used. It means data is sent several bits over several wires or channels at the same time.
- Universal serial bus (USB) is used for sending data externally (between devices).
- In USB, serial data transmission is used. It means data is sent one bit at a time over a single wire or channel.

Question 2:

Priya stores her website on a webserver. To transmit the website data to the webserver she uses parallel duplex data transmission. Describe how data is transmitted using parallel duplex data transmission. (4)

- It allows several/multiple bits to be transmitted simultaneously.
- Several/multiple wires are used for transmission of data.
- Moreover, data is transmitted in both directions at the same time.

Question 3:

A file server is used as a central data store for a network of computers. Rory sends data from his computer to a file server that is approximately 100 metres away. It is important that the data is transmitted accurately. Rory needs to be able to read data from and write data to the file server at the same time.

Identify the most suitable data transmission methods for this application: (2)

Method 1	Tick	Method 2	Tick
Serial	✓	Simplex	
Parallel		Half-duplex	
		Duplex	✓

Explain why your answer is the most suitable data transmission. (4)

- Serial duplex is used since serial uses a single wire hence there is a less chance of interference.
- It is more reliable over longer distances (100 metres and above).
- It is more accurate and bits won't be skewed over a long distance.
- Moreover, duplex transmits data in both directions simultaneously which allows read and write operations at the same time.
- Read and write at the same time won't be allowed by other methods such as simplex and half-duplex.

Question 5:

A company has over 100 cameras. At the end of each day all these cameras send their images, capture over the last 24 hours, to a central computer.

Explain why a company uses dedicated fibre optic cable rather than transmitting the data over the local broadband network? (2)

- Data is transmitted more securely because it is a dedicated line.
- Fibre optic is not only more reliable than local broadband but it also transmits data at a faster rate.

Question 6:

(a) State what is meant by the terms:

Parallel data transmission .....

.....

.....

Serial data transmission .....

.....

.....

[2]

(b) Give **one** benefit of each type of data transmission.

Parallel data transmission

Benefit .....

.....

Serial data transmission

Benefit .....

.....

[2]

(c) Give **one** application of each type of data transmission. Each application must be different.

Parallel data transmission

Application .....

.....

Serial data transmission

Application .....

.....

[2]

Answer:

(a) parallel

any **one** from:

– 8 bits/1 byte/multiple bits sent at a time
– using many/multiple/8 wires/lines (1 mark)

serial

any **one** from:

– one bit sent at a time
– over a single wire (1 mark) [2]

(b) parallel

– faster rate of data transmission (1 mark)

serial

any **one** from:

– more accurate/fewer errors <u>over a longer distance</u>
– less expensive wiring
– less chance of data being skewed/out of synchronisation/order (1 mark) [2]

(c) parallel

any **one** from:

– sending data from a computer to a printer
– internal data transfer (buses) (1 mark)

serial

– connect computer to a modem (1 mark) [2]

Question 7:

(a) **Three** descriptions of data transmission are given below.

Tick (✓) the appropriate box in each table to show the:

- type of transmission
- method of transmission

Description 1:

Data is transmitted several bits at a time down several wires in both directions simultaneously.

Type	Tick (✓)
simplex	
half-duplex	
full-duplex	

Method	Tick (✓)
serial	
parallel	

Description 2:

Data is transmitted in one direction only, one bit at a time, down a single wire.

Type	Tick (✓)
simplex	
half-duplex	
full-duplex	

Method	Tick (✓)
serial	
parallel	

Description 3:

Data is transmitted one bit at a time down a single wire; the data is transmitted in both directions but not at the same time.

Type	Tick (✓)
simplex	
half-duplex	
full-duplex	

Method	Tick (✓)
serial	
parallel	

[6]

Answer:

(a)

Type	Tick (✓)
simplex	
half-duplex	
full-duplex	✓

Method	Tick (✓)
serial	
parallel	✓

Type	Tick (✓)
simplex	✓
half-duplex	
full-duplex	

Method	Tick (✓)
serial	✓
parallel	

Type	Tick (✓)
simplex	
half-duplex	✓
full-duplex	

Method	Tick (✓)
serial	✓
parallel	

[6]

Question 8:

Maisey purchases a new router and attaches it to her computer. The connection she sets up uses duplex data transmission.

(a) **Five** statements are given about duplex data transmission.

Tick (✓) to show if the statement is **True** or **False**.

Statement	True (✓)	False (✓)
Duplex data transmission can be either serial or parallel		
Duplex data transmission is when data is transmitted both ways, but only one way at a time		
Duplex data transmission is always used to connect a device to a computer		
Duplex data transmission is when data is transmitted both ways at the same time		
Duplex data transmission automatically detects any errors in data		

[5]

Answer:

Question	Answer	Marks
9(a)	**One** mark per each correct tick	5

Statement	True (✓)	False (✓)
Duplex data transmission can be either serial or parallel	✓	
Duplex data transmission is when data is transmitted both ways, but only one way at a time		✓
Duplex data transmission is always used to connect a device to a computer		✓
Duplex data transmission is when data is transmitted both ways at the same time	✓	
Duplex data transmission automatically detects any errors in data		✓

Question 9:

Use the list given to complete Blair's paragraph by inserting the correct **five** missing terms. Not all terms will be used. Terms can be used more than once.

- duplex
- half-duplex
- parallel
- serial
- simplex

..... data transmission is when data is transmitted a single bit at a time. ..... data transmission is when multiple bits of data are sent all at once. If a user wants to transmit data over a long distance, with the highest chance of accuracy, ... data transmission should be used. If data needs to be transmitted in one direction only, for example from a computer to a printer, ... data transmission should be used. If a user has a large amount of data to transmit and this needs to be done as quickly as possible ..... data transmission should be used.

[5]

Answer:

Question	Answer	Marks
3	**One** mark for each correct term in the correct order Serial Parallel Serial Simplex Parallel	**5**

Question 10:

(a) **Six** statements are given about methods of data transmission.

Tick (✓) to show if each statement applies to serial simplex, parallel simplex, parallel half-duplex or serial duplex data transmission. Some statements may apply to more than **one** data transmission method.

Statement	Serial simplex (✓)	Parallel simplex (✓)	Parallel half-duplex (✓)	Serial duplex (✓)
bits are transmitted along a single wire				
data is transmitted in both directions				
it is only suitable for distances less than 5 metres				
bits from the same byte are transmitted one after the other				
data may **not** arrive in the correct sequence				
data is transmitted in both directions, but only **one** direction at a time				

[6]

Answer:

Question	Answer	Marks
3(a)	**One** mark per each correct row.	6

Statement	Serial simplex (✓)	Parallel simplex (✓)	Parallel half-duplex (✓)	Serial duplex (✓)
bits are transmitted along a single wire	✓			✓
data is transmitted in both directions			✓	✓
it is only suitable for distances less than 5 metres		✓	✓	
Bits from the same byte are transmitted one after the other	✓			✓
data may **not** arrive in the correct sequence		✓	✓	
data is transmitted in both directions, but only **one** direction at a time			✓	

Question 11:

(c) The type of data transmission between the computer and the printer is serial half-duplex data transmission.

(i) Describe how data is transmitted using serial half-duplex data transmission.

.....

.....

.....

.....

.....

.....

.....

..... [4]

(ii) Explain why the data transmission needs to be half-duplex rather than simplex.

.....

.....

.....

..... [2]

Answer:

Question	Answer	Marks
4(c)(i)	**Four** from: – Bits sent **one at a time** – … down a single wire – Data sent in both directions … – … but only one direction at a time	**4**
4(c)(ii)	Any **two** from: – Simplex only sends data in one direction – … so, printer may not be able to tell computer an error has occurred, and computer may not be able to send printer the document to be printed **NOTE:** Award any valid contextual answer for MP2	**2**

Question 12:

A school network is used to transmit and store data about students.

(a) Different types and methods of transmission can be used to send data across the network.

Three descriptions about data transmission are given.

Tick (✓) **one Method** and tick (✓) **one Type** for each description.

Description	Method		Type		
	Serial (✓)	Parallel (✓)	Simplex (✓)	Half-duplex (✓)	Duplex (✓)
Data is sent down a single wire in a single direction only.					
Data is sent down multiple wires in both directions, at the same time.					
Data is sent down a single wire in both directions, but never at the same time.					

[3]

Answer:

Question	Answer	Mark
2(a)	1 mark per each correct row:	3

Description	Method		Type		
	Serial (✓)	Parallel (✓)	Simplex (✓)	Half-duplex (✓)	Duplex (✓)
Data is sent down a single wire in a single direction only.	✓		✓		
Data is sent down multiple wires in both directions, at the same time.		✓			✓
Data is sent down a single wire in both directions, but never at the same time.	✓			✓	

2.1.3 Universal Serial Bus (USB):

- It is an asynchronous serial data transmission method.
- It uses serial transmission so bits of data are sent one at a time.
- It is a Universal standard used for transfer of data between a computer and devices.
- The USB allows both half-duplex and full-duplex data transmission.

Structure of USB cable:

- A four-wire shielded cable.
- Two of the wires are used for power and earth; other two are used in data transmission.

When a device is plugged into a computer using USB port:

- The computer automatically detects the presence of device due to slight change in voltage level.
- The device is automatically recognized, and the appropriate device driver is loaded.
- If a new device is detected, the computer looks up the device driver which matches the device; if it's unavailable, the user is prompted to download the appropriate software.

Advantages of USB Systems (fully detailed):

Exam Tip:

1. Memorize any four of the advantages and use them when the question demands an explanation of any number of advantages.
2. If question simply demands stating of advantages (no explanation), then write according to marks by summarizing the following given points.

1. The devices are automatically detected and configured when initially attached due to changes in voltage level.
2. It is a universal standard so it is likely to be compatible with every computer.
3. It is impossible to connect device incorrectly as connector only fits one way.
4. It is a high-speed connection so data will be transmitted quicker.
5. It uses serial transmission so it is cheaper to manufacture/buy and less chance of skewing of data.
6. It doesn't require a wireless network therefore, can be used if a network is down.
7. It is backwards compatible (with earlier versions of USB ports) so no additional technology is needed.
8. It can power the device therefore no separate source of power is needed.
9. The drivers are automatically downloaded so there is no need to find them online or install manually.

Disadvantages of USB Systems:

1. The maximum cable length is presently about 5 metres.
2. The present transmission rate is limited to less than 500 megabits per second.
3. The older USB standard (e.g. 1.1) may not be supported in near future.

USB-C System:

- USB-C is a new type of USB connector which has now become more common in laptops and tablets/phones.
- It is a 24-pin symmetrical connector which means it will fit into a USB-C port either way round.
- It is expected to become the new industry standard (universal) format.

Advantages of USB-C:

1. It is much smaller and thinner than older USB connectors
2. It offers 100 watt (20 volt) power connectivity, which means full-sized devices can now be charged
3. It can carry data at 10 gigabits per second (10 Gbps) which means it can now support 4K video delivery.
4. USB-C is backward compatible (to USB 2.0 and 3.0) provided a suitable adaptor is used.

Exam Style Questions:

Question 1:

Nadia purchases a printer to print out her homework.

She connects the printer to her computer using USB.

(a) Explain what is meant by USB.

.....

.....

.....

.....

.....

..... [3]

Answer:

Question	Answer	Marks
6(a)	**Three** from: – Universal Serial Bus – Data transmission method – Uses serial transmission // bits of data are sent one at a time – Universal standard // common interface	3

Question 2:

(c) A computer includes an Integrated Circuit (IC) and a Universal Serial Bus (USB) for data transmission.

Describe how the computer uses these for data transmission, including the type of data transmission used.

IC .....

.....

.....

.....

USB .....

.....

.....

.....

[4]

Answer:

7(c)	2 marks for IC, 2 marks for USB **IC** • parallel transmission // description of parallel • for sending data internally **USB** • serial transmission // description of serial • for sending data externally (to and from peripherals / between devices)	**4**

Question 3:

Carla's computer has a USB port.

Carla uses the USB port to connect her mobile device to her computer, to transfer her photos.

(a) Give **three** benefits of using a USB port to connect the mobile device to the computer.

Benefit 1 .....

.....

Benefit 2 .....

.....

Benefit 3 .....

.....

[3]

(b) State the type of data transmission used when transferring data using a USB port.

..... [1]

Answer:

Question	Answer	Marks
3(a)	Any **three** from: – It is a universal standard – It can't be inserted the wrong way around – Supports different transmission speeds – Automatically detects if correct driver installed – It will charge the mobile device at the same time	3

Question	Answer	Marks
3(b)	– Serial	1

Question 4:

Arjun uses a scanner to create digital versions of some printed documents.

The scanner is attached to his computer using a USB connection.

(a) Tick (✓) to show if the USB connection uses **Parallel** or **Serial** data transmission.

Describe your chosen method of data transmission.

Parallel ☐

Serial ☐

Description

.....

.....

.....

.....

[3]

Answer:

Question	Answer	Marks
5(a)	**One** mark for correct tick, **two** marks for description – Serial – Bits sent one at a time – Single wire If parallel given, no mark for parallel, but follow through for correct description of parallel: – Multiple bits sent at a time – Multiple wires	3

2.2 | Methods of Error Detection

2.2.1 Checking for Errors:

The errors can occur during data transmission due to:

1. Interference as all types of cable can suffer from electrical interference, which can cause data to be corrupted or even lost.
2. Problems during packet switching which can lead to data loss or data gain
3. Skewing of data which occurs during parallel data transmission can cause data corruption if the bits arrive out of synchronization.

There are a number of error detection methods for detecting errors in data after transmission:

1. Parity checks (odd and even), including parity byte & parity block check
2. Checksum
3. Echo Check

2.2.2 Parity Checks, Checksum & Echo Check:

1) Parity Checks:

- It checks a byte of data, and the parity can be set to odd or even.
- The sender and receiver agree on the parity to be used (agreement).
- The data is split into bytes (blocks of 7 bytes).
- The sender counts the number of 1s & 0s in each byte and each byte is assigned a parity bit to be transmitted with it to match the even or odd parity used.
- The receiving device recounts the number of 1s & 0s in each byte and compares them to the even or odd parity being used.
- If it does not match the parity, an error is reported/identified.
- In a block check, the location of the error(s) can be identified at the intersection.

Question: Describe a situation in which a parity check cannot detect corruption of a byte OR describe a situation in which an error during parity check goes undetected.

1. Error will not be detected if there are multiple errors in same byte that still produce the same parity bit.
2. It will not be detected if an even/odd number of digits are changed (depending upon even/odd parity used).
3. It will not be detected if a transposition error has occurred.

Practical Method/Approach of Parity Byte Checking:

> **NOTE:** The following steps explain the way of solving practical parity checking questions asked in examination mostly. Theoretical knowledge of parity checking given above is rarely asked.

1) Systems that use **EVEN PARITY** have an **even number of 1- bits**; systems that use **ODD PARITY** have an **odd number of 1-bits**.

2) If it is given in a question that **even parity** is used and an **incomplete register** like below is given, you need to **count the number of 1's** to see if they are **even or odd**. If they are **even** already, then **simply add 0's** in the blank space. If **1's are odd**, then you need to **balance** and **write 1's** until the **total number** of **1's become even**.

	Parity bit							
Register A		0	1	0	0	1	0	1

3) Similarly, if it is given in a question that **odd parity** is used and an **incomplete register** like above is given, you need to **count the number of 1's** to see if they are **even or odd**. If they are **odd** already, then **simply add 0's** in the blank space. If **1's are even**, then you need to **balance** and **write 1's** until the **total number** of **1's become odd**.

4) If the examiner gives you a **complete register filled with 8 bits**, and tells you that **even parity** is used, asking you to **identify if the data was transmitted correctly**. You simply need to **count** the **number of 1's** in the register and **check if they are even**. If they are **even,** then data was **transmitted correctly** and if they are **odd** then it was **corrupted during transmission**.

5) Similarly, if the examiner gives you a **complete register filled with 8 bits**, and tells you that **odd parity** is used, asking you to **identify if the data was transmitted correctly**. You simply need to **count** the **number of 1's** in the register and **check if they are odd**. If they are **odd** then data was **transmitted correctly** and if they are **even** then it was **corrupted during transmission**.

Practice Questions:

Q1. 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
1 1 0 0 1 0 0 0		
0 1 1 1 1 1 0 0		
0 1 1 0 1 0 0 1		

Q2. A system uses odd parity.

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

Received byte	Byte transmitted correctly	Byte transmitted incorrectly
1 0 1 1 0 1 0 0		
0 1 1 0 1 1 0 1		
1 0 0 0 0 0 0 1		

Q3. Parity checks are often used to detect errors that may occur during data transmission.

The received bytes in the table below were transmitted using **odd parity**.

Tick (✓) to show whether each byte has been **corrupted during transmission** or **not corrupted during transmission**.

Received byte	corrupted during transmission (✓)	not corrupted during transmission (✓)
10110100		
01101101		
10000001		

[3]

Q4. A system uses **even parity**. Write the appropriate parity bit for each byte.

Parity Bit							
	1	0	1	0	0	1	1
	1	0	1	1	1	1	1
	1	0	1	0	0	0	1

[2]

Q5. Tick (✓) to show whether an **Even** or an **Odd** parity check has been used for each binary value.

8-bit binary value	Even (✓)	Odd (✓)
11111111		
01100110		
01111011		
10000000		

[4]

Q6. Identify whether each 8-bit binary value has been sent using odd or even parity by writing odd or even in the type of parity column.

8-bit binary value	Type of parity
01100100	
10010001	
00000011	
10110010	

[4]

Practical Method/Approach of Parity Block Checking:

In this method, a block of data is sent, and the number of 1-bits are totaled horizontally and vertically (in other words, a parity check is done in both horizontal and vertical directions).

As the following example shows, this method not only identifies that an error has occurred but also indicates where the error is.

To solve questions like the following:

When eight bytes of data have been collected, they are transmitted to a computer 100 km away. Parity checks are carried out to identify if the data has been transmitted correctly. The system uses **even parity** and column 1 is the parity bit.

The eight bytes of data are sent together with a ninth parity byte:

	parity bit	column 2	column 3	column 4	column 5	column 6	column 7	column 8
byte 1	1	0	0	0	0	1	0	0
byte 2	1	1	1	1	0	0	1	1
byte 3	0	1	0	0	1	0	0	0
byte 4	0	1	1	1	0	0	0	1
byte 5	1	0	0	0	1	1	1	1
byte 6	0	0	0	0	0	0	0	0
byte 7	1	1	1	0	1	0	0	0
byte 8	1	0	0	0	1	1	1	0
parity byte	1	0	1	1	0	1	1	1

(i) Identify which of the eight bytes contains an error.

byte .....[1]

(ii) Identify which column contains an error.

column .....[1]

This example uses even parity.

1) First we need to see **what type of parity** is used.

2) According to the even/odd parity used, we need to **count 1's** in all **columns** and check which of the column **does not follow** the **even/odd parity** used.

3) Then we need **to count 1's** in all **bytes** (rows) and check which of the rows **does not follow** the **even/odd parity** used.

4) The **intersection point** of that column and byte gives the **corrupted bit**.

5) If the examiner asks you to **circle** the corrupted bit, then simply encircle the bit at the intersection point.

6) If the examiner asks you to **write byte number and column number**, simply write the byte number with wrong parity and the column number with wrong parity in the provided space.

	parity bit	column 2	column 3	column 4	column 5	column 6	column 7	column 8
byte 1	1	0	0	0	0	1	0	0
byte 2	1	1	1	1	0	0	1	1
byte 3	0	1	0	0	1	0	0	0
byte 4	0	1	1	1	0	0	0	1
byte 5	1	0	0	0	1	1	1	1
byte 6	0	0	0	0	0	0	0	0
byte 7	1	1	1	0	1	0	0	0
byte 8	1	0	0	0	1	1	1	0
parity byte	1	0	1	1	0	1	1	1

(i) Identify which of the eight bytes contains an error.

byte **5** .....[1]

(ii) Identify which column contains an error.

column **4** .....[1]

(iii) How did you arrive to your answer in part (i)(ii)? (2)

- Column 4 has odd number of 1's (3 ones).
- Byte 5 has odd number of 1's (5 ones).

The corrupted bit has been encircled as well for you to understand (though it is not the requirement of this question)

Exam Style Questions:

Question 1:

Nine bytes of data are transmitted from one computer to another. Even parity is used. An additional parity byte is also sent.

The ten bytes arrive at the destination computer as follows:

	parity bit	bit 2	bit 3	bit 4	bit 5	bit 6	bit 7	bit 8
byte 1	1	1	1	0	1	1	1	0
byte 2	0	0	0	0	0	1	0	1
byte 3	0	1	1	1	1	0	0	0
byte 4	1	1	0	0	0	0	0	0
byte 5	1	0	1	1	1	1	1	0
byte 6	0	1	0	1	1	0	0	1
byte 7	0	1	1	1	0	0	1	1
byte 8	0	0	1	1	0	1	1	0
byte 9	1	1	0	0	0	0	1	1
parity byte	0	0	1	0	0	0	1	0

One of the bits was corrupted during the data transmission.

(a) **Circle** the corrupt bit in the corrupt byte in the table above. [1]

(b) Explain how the corrupted bit was found.

.....

.....

.....

.....

.....

.....[2]

Answer:

(a) Intersection of Row 7 and column 4 circled [1]

(b) – Row (byte number) 7 has an odd number of 1s (five 1s)
– Column (bit number) 4 has an odd number of 1s (five 1s)

[2]

Question 2:

The three binary numbers in the registers A, B and C have been transmitted from one computer to another.

	Parity bit							
Register A	1	0	0	1	1	0	0	0
Register B	0	1	1	0	0	1	1	1
Register C	1	0	0	1	1	0	0	1

One binary number has been transmitted incorrectly. This is identified through the use of a parity bit.

Identify which register contains the binary number that has been transmitted **incorrectly**. Explain the reason for your choice.

The binary number that has been transmitted incorrectly is in **Register** .....

Explanation .....

.....

.....

.....

.....

.....

[4]

Answer:

Register C

- Count the number of 1 bits in each byte/register.
- Two registers have an odd number of 1 bits (odd parity).
- Odd parity must be the parity used.
- One register has an even number of 1 bits (even parity).
- One with an even number of one bits is incorrect.
- Register C should have odd parity.

Question 3:

The three binary numbers in the registers X, Y and Z have been transmitted from one computer to another.

								Parity bit
Register X	1	0	0	1	0	0	1	0
Register Y	1	1	1	0	0	1	1	1
Register Z	1	1	1	0	1	0	0	1

Only **one** binary number has been transmitted correctly. This is identified through the use of a parity bit.

Identify which register contains the binary number that has been transmitted **correctly**. Explain the reason for your choice.

The binary number that has been transmitted correctly is in **Register** .....

Explanation .....

.....

.....

.....

.....

.....

[4]

Answer:

Register Y

- Count the number of 1 bits in each byte/register.
- Two registers have an odd number of 1 bits (odd parity).
- Even parity must be the parity used.
- One register has an even number of 1 bits (even parity).
- The two registers with an odd number of one bits is incorrect.
- Register X and Z should have even parity.

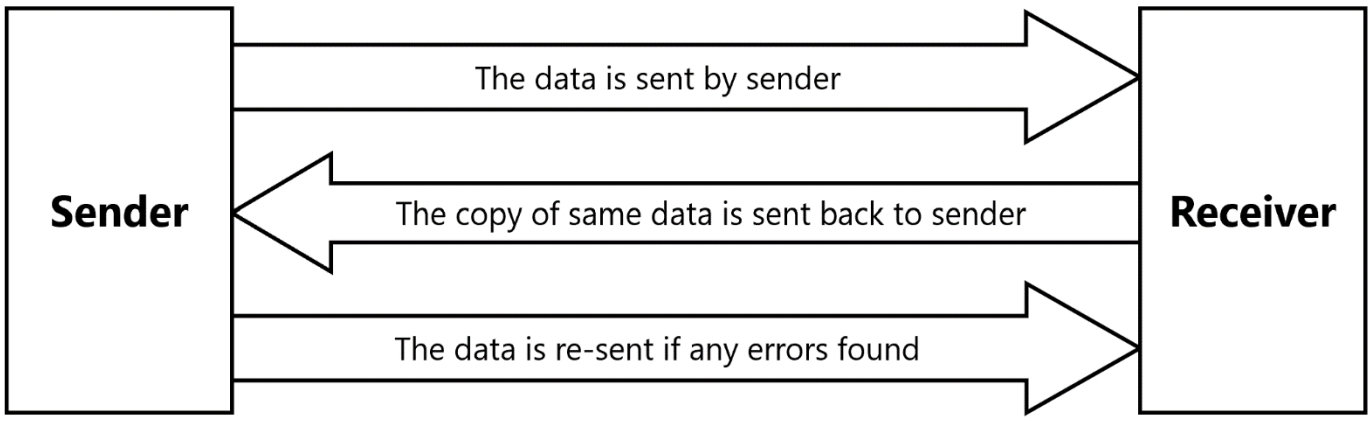
2) Checksum:

- Before transmission, calculation is performed on data to get an additional value called checksum using an algorithm.
- The value is then transmitted with the block of data.
- The value is recalculated by the receiver using same algorithm on the block of data received.
- A comparison is made between checksum values before and after transmission.
- If checksum values are different, then error is detected, and retransmission request is sent.
- If checksum values are the same, then data has been transmitted correctly.

3) Echo Check:

- When data is sent to another device, a copy of the data is sent back to the sender.
- The returned data is compared with the original data by the sender's computer.
- If there are no differences, then the data was sent without error.
- If the two sets of data are different, then an error occurred at some stage during the data transmission.
- It is not very reliable because if both sets of data are different, it is not known whether the error occurred while sending the data in first place, or when sending the data back for checking to the sender.

The following diagram shows the process of echo check:



2.2.3 Check Digits:

- They are used to identify errors in data entry caused by mistyping or mis-scanning a barcode.
- They are used for barcodes on products, such as International Standard Book Numbers (ISBN)(found on the cover of a book) and Vehicle Identification Numbers (VIN).

They can usually detect the following types of error:

1. An incorrect digit being entered (such as 5327 entered instead of 5307).
2. Transposition error where two numbers have changed order (such as 5037 instead of 5307).
3. Digits being omitted or extra digits (such as 537 instead of 5307 or 53107 instead of 5307).
4. Phonetic errors (such as 13 (thirteen), instead of 30 (thirty).

Process of Check Digit:

- It is an additional digit that is calculated from the data.
- It is then added to the data.
- The digit is recalculated when data is entered.
- Both digits are compared to check for error.
- If digits are different, error is detected.
- If digits match, no error is detected.

There are a number of different methods used to generate a check digit. Two common methods will be considered here:

1. ISBN 13
2. Modulo-11

NOTE: You will not need to remember the steps shown in following algorithms as the steps will be given to you in the question. However, it is important that you understand how to use an algorithm to calculate or verify check digits. Therefore, study the following examples & calculations very carefully so you can learn how to apply these steps.

1) ISBN 13:

- As the '13' in the ISBN 13 suggests, the check digit in ISBN 13 is the thirteenth digit in the number.
- This 13^{th} digit (check digit) is generated from the other 12 digits in the number.

Steps of Calculation (without check digit):

1. Add all the odd numbered digits together.
2. Add all the even numbered digits together and multiply the result by 3.
3. Add the results from Step 1 & Step 2 together and divide by 10.
4. Take the remainder, if it is zero then use this value, otherwise subtract remainder from 10 to find the check digit.

Example Calculation 1: Generation of the check digit from the other 12 digits in a number

We will use the following sample barcode (ISBN 13 code with check digit):

- The first 12 digits in this barcode are: **9 7 8 0 3 4 0 9 8 3 8 2**
- We will now use the first 12 digits to calculate the 13th check digit given below.
- The last 13th digit in this barcode is: **9 (which is the check digit)**

9	**7**	**8**	**0**	**3**	**4**	**0**	**9**	**8**	**3**	**8**	**2**
odd	even	odd	even	odd	even	odd	even	odd	even	odd	even
Step 1 – 9 + 8 + 3 + 0 + 8 + 8 = 36											
Step 2 – 3 x (7 + 0 + 4 + 9 + 3 + 2) = 3 x (25) = 75											
Step 3 – (36 + 75)/10 = (111)/10 = 11 remainder 1											
Step 4 – 10 – 1 = **9 (the check digit)**											

- The calculated thirteenth digit is 9.
- Writing it together, we end up with the thirteen-digit number **9 7 8 0 3 4 0 9 8 3 8 2 9** which matches the number in barcode.

To check that an ISBN 13-digit code is correct, including its check digit, similar steps are followed.

Steps of Recalculation (including check digit):

1. Add all the odd numbered digits together, **including the check digit**.
2. Add all the even numbered digits together and multiply the result by 3.
3. Add the results from Step 1 & Step 2 together and divide by 10.
4. The number is correct if the remainder is 0 (zero).

Example Calculation 2: Re-calculation of the check digit from the thirteen-digit number (which now includes the check digit)

We will use the same following barcode (ISBN 13 code with check digit):

- The 13 digits in this barcode are: **9 7 8 0 3 4 0 9 8 3 8 2 9 (including check digit)**
- We will now use these 13 digits to confirm if the check digit is correct.

9	**7**	**8**	**0**	**3**	**4**	**0**	**9**	**8**	**3**	**8**	**2**	**9**
odd	even	odd	even	odd	even	odd	even	odd	even	odd	even	odd
Step 1 – 9 + 8 + 3 + 0 + 8 + 8 + 9 = 45												
Step 2 – 3 x (7 + 0 + 4 + 9 + 3 + 2) = 3 x (25) = 75												
Step 3 – (45 + 75)/10 = (120)/10 = 12 remainder 0												
Step 4 – The number is correct because the **remainder is 0**												

2) Modulo-11:

- This method can have different lengths of number which makes it suitable for many applications, such as product codes or VINs.

Steps of Calculation:

The following algorithm is used to generate the check digit for a number with seven digits:

1. Each digit in the number is given a weighting of 8, 7, 6, 5, 4, 3, or 2 starting from the left (weightings start from 8 since the number will become eight-digit when the check digit is added).
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.
4. The remainder is then subtracted from 11 which gives the value of check digit and if the remainder is 10 then check digit 'X' is used.

Example Calculation 1: Generation of the check digit from the other digits in a number

The example to be used has the following seven-digit number: **4 1 5 6 7 1 0**
The second row contains the weighting values for each digit in the table given below:

4	**1**	**5**	**6**	**7**	**1**	**0**
8	7	6	5	4	3	2
Step 1 – Each digit is given weightings starting from left, e.g. digit 4 has weighting 8 and so on.						
8 x 4 = 32	**7 x 1 = 7**	**6 x 5 = 30**	**5 x 6 = 30**	**4 x 7 = 28**	**3 x 1 = 3**	**2 x 0 = 0**
Step 3 – (32 + 7 + 30 + 30 + 28 + 3 + 0) = 130 130/11 = 11 remainder 9						
Step 4 – 11 – 9 = **2 (check digit)**						

- Therefore, we end up with the eight-digit number **4 1 5 6 7 1 0 2.**

To check that the eight-digit number is correct, including its check digit, similar steps are followed.

Steps of Recalculation (including check digit):

1. Each digit in the number is given a weighting of 8, 7, 6, 5, 4, 3, 2 or 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.
4. The number is correct if the remainder is 0 (zero)..

Example Calculation 2: Re-calculation of the check digit from the eight-digit number (which now includes the check digit)

The example to be used has the following eight-digit number: **4 1 5 6 7 1 0 2**
The second row contains the weighting values for each digit in the table given below:

4	**1**	**5**	**6**	**7**	**1**	**0**	**2**
8	7	6	5	4	3	2	1
Step 1 – Each digit is given weightings starting from left, e.g. digit 4 has weighting 8 and so on.							
8 x 4 = 32	**7 x 1 = 7**	**6 x 5 = 30**	**5 x 6 = 30**	**4 x 7 = 28**	**3 x 1 = 3**	**2 x 0 = 0**	**1 x 2 = 2**
Step 3 – (32 + 7 + 30 + 30 + 28 + 3 + 0 + 2) = 132 132/11 = 12 remainder 0							
Step 4 – The number is correct because the **remainder is 0**							

Practice Questions

Q1. Check digits are used to ensure the accuracy of input data.

A 7-digit code number has an extra digit on the right, called the check digit.

Digit position	1	2	3	4	5	6	7	8
Digit	–	–	–	–	–	–	–	–

The check digit is calculated as follows:

- each digit in the number is multiplied by its digit position
- the seven results are then added together
- this total is divided by 11
- the remainder gives the check digit (if the remainder = 10, the check digit is X)

(i) Calculate the check digit for the following code number. Show all your working.

4 2 4 1 5 0 8 …

.....

.....

.....

Check digit .....

[2]

(ii) An operator has just keyed in the following code number:

3 2 4 0 0 4 5 X

Has the operator correctly keyed in the code number?

.....

Give a reason for your answer.

.....

.....

.....

.....

[2]

Q2. Check digits are used to ensure the accuracy of entered data.

A 7-digit number has an extra digit on the right, called the check digit.

digit position:	1	2	3	4	5	6	7	8
digit:	–	–	–	–	–	–	–	–

↑ check digit

The check digit is calculated as follows:

- each digit in the number is multiplied by its digit position
- the seven results are then added together
- this total is divided by 11
- the remainder gives the check digit (if the remainder = 10, the check digit is X)

(a) Calculate the check digit for the following number. Show all your working.

4 2 4 1 5 0 8 ...

.....

.....

.....

Check digit .....

[2]

(b) An operator has just keyed in the following number:

3 2 4 0 0 4 5 X

Circle below **correct** if the check digit is correct **OR incorrect** if the check digit is incorrect.

correct **incorrect**

Explain your answer.

.....

.....

.....

.....

[3]

2.2.4 Automatic Repeat Query (ARQ):

- They are used to establish that data is received without error.

It is also known as Automatic Repeat Request (ARQ).

Process of Automatic Repeat Query (ARQ):

- It uses acknowledgment and timeout.
- The sender starts a timer when data is transmitted, and a request is sent with data requiring acknowledgment.
- The receiver uses an error checking method (e.g., error detected by parity check or check sum) to check whether the data has been received accurately.
- If no error is detected, then a positive acknowledgment is sent back to the sender.
- If an error is detected, then negative acknowledgment is sent back to the sender and a request is automatically sent to resend data.
- If the sender gets no acknowledgment within the set time, it resends the data.
- Resend requests are repeatedly sent until data is received correctly or limit is reached.

Positive Acknowledgment:	**Negative Acknowledgment:**
It is a message sent by the receiver indicating that data has been received correctly.	It is a message sent by the receiver indicating that data has been received incorrectly.

Timeout:

- It is the time allowed to elapse before an acknowledgment is received.

Exam Style Questions:

Question 1:

A library's archive system uses an error detection and correction system that combines a parity check with an automatic repeat request (ARQ)

Describe how this system uses the parity check and ARQ. (6)

- The system could use either odd or even parity.
- A parity bit is added to the byte of data.
- Each byte is checked after transmission to see if it matches the odd/even parity used as numbers of 1's are counted.
- If parity is correct, no error is found.
- An acknowledgment is sent that data is received correctly and the next packet of data is transmitted.
- If parity is incorrect, an error is detected and a request is automatically sent to resend data.
- Resend request is repeatedly sent until data is received correctly or limit is reached.

Exam Tip:

- Each error-checking method is asked for no more than 4 marks in an exam.
- The examiner can either give a specific error-checking method alone for 4 marks or ask you to write any one of your choices.

If methods are combined, then examiner can ask in following ways:

Question 2:

There are various methods used to detect errors that can occur during data transmission and storage.

Describe each of the following error detection methods: [8]

1) Parity check

2) Check digit

3) Checksum

4) Automatic Repeat request (ARQ)

Exam Tip:

- Since 4 methods are asked and 8 marks are assigned, each method will be answered for no more than 2 marks so (2 x 4 = 8 marks).

Question 3:

Data can sometimes be corrupted when it is transmitted from one computer to another, causing errors to be present in the data.

Identify and describe three methods of error detection that could be used to see if an error has occurred. [9]

> **Exam Tip:**
>
> - Since 3 methods are asked and 9 marks are assigned, each method will be answered for no more than 3 marks so (3 x 3 = 9 marks).

Question 4:

Five statements are given about error-checking methods.

(a) Tick (✓) to show whether each statement applies to Automatic Repeat reQuest (ARQ), check digit or checksum. Some statements may apply to more than **one** error-checking method.

Statement	ARQ (✔)	Check digit (✔)	Checksum (✔)
checks for errors on data entry			
uses a process of acknowledgement and timeout			
compares **two** calculated values to see if an error has occurred			
may resend data until it is confirmed as received			
checks for errors in data after transmission from a computer to another			

[5]

(b) Identify **one** other error-checking method.

..... [1]

Answer:

<table>
<tr><th>Question</th><th>Answer</th><th>Marks</th></tr>
<tr><td>3(a)</td><td>One mark per each row
<table>
<tr><th>Statement</th><th>ARQ (✓)</th><th>Check digit (✓)</th><th>Checksum (✓)</th></tr>
<tr><td>checks for errors on data entry</td><td></td><td>✓</td><td></td></tr>
<tr><td>uses a process of acknowledgement and timeout</td><td>✓</td><td></td><td></td></tr>
<tr><td>compares two calculated values to see if an error has occurred</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>may resend data until it is confirmed as received</td><td>✓</td><td></td><td></td></tr>
<tr><td>checks for errors in data after transmission from a computer to another</td><td></td><td></td><td>✓</td></tr>
</table></td><td>5</td></tr>
<tr><td>3(b)</td><td>– Parity check</td><td>1</td></tr>
</table>

Question 5:

(a) Companies use error detection methods to make sure that data is accurate.

One error detection method is the use of a check digit.

Explain what is meant by a check digit and how it is used to detect errors.

.....

.....

.....

.....

.....

.....

.....

..... [4]

Answer:

Question	Answer	Marks
10(a)	**Four** from: Validation method Used to check data entry Digit is calculated from data // by example Digit is appended / added to data Digit is recalculated when data has been input Digits are compared If digits are different, error is detected // If digits match, no error is detected	4

Question 6:

(b) The data will also be checked using a checksum.

Describe how a checksum can be used to check that the data has been transmitted correctly.

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [5]

Answer:

2(b)	Any **five** from: – A value is calculated **from the data** – The value is calculated **using an algorithm** // by example – The value is appended to the data to be transmitted – Value is recalculated after transmission – Values are compared – If the values match the data is correct // if the values do not match the data is incorrect	5

Question 7:

Five statements are given about the error-checking methods checksum, check digit and parity check.

(a) Tick (✓) to show whether each statement applies to checksum, check digit or parity check. Some statements may apply to more than **one** error-checking method.

Statement	Checksum (✓)	Check digit (✓)	Parity check (✓)
uses an additional bit to create an odd or even number of 1s			
checks for errors on data entry			
compares **two** calculated values to see if an error has occurred			
will **not** detect transposition errors			
sends additional values when data is transmitted from a computer to another			

[5]

Answer:

Question	Answer	Marks
3(a)	**One** mark per each correct row.	**5**

Statement	Checksum (✓)	Check digit (✓)	Parity check (✓)
uses an additional bit to create an odd or even number of 1s			✓
checks for errors on data entry		✓	
compares **two** calculated values to see if an error has occurred	✓	✓	
will **not** detect transposition errors			✓
sends additional values when data is transmitted from one computer to another	✓		(✓)

2.3 | Encryption

2.3.1 Purpose of Encryption:

When data is transmitted over any public network (wired or wireless), there is always a risk of it being intercepted by, for example, a hacker.

Under these circumstances, a hacker is often referred to as an eavesdropper. The use of encryption helps to minimize this risk.

Why is encryption used?

- It is used so that data cannot be understood if intercepted without the decryption key.

Encryption:

- It is scrambling for data to make it meaningless.
- It uses an encryption algorithm and key to encrypt data and decryption key to decipher encrypted message.
- Encryption is used primarily to protect data in case it has been hacked while encryption won't prevent hacking, it simply makes the data meaningless to the eavesdropper unless the recipient has the necessary decryption tools.
- This is particularly important if the data is sensitive or confidential such as credit card/bank details, medical history, or legal documents etc.

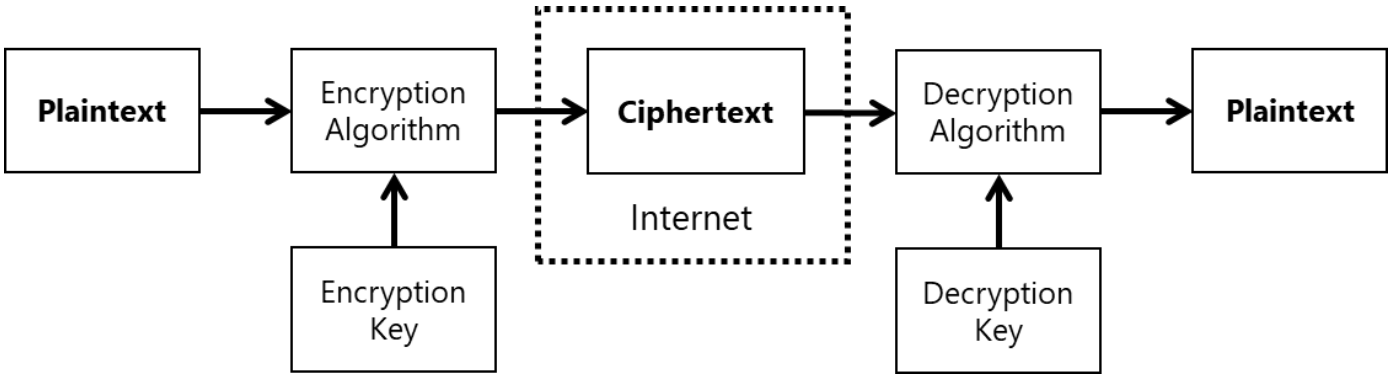
Plain Text & Cipher Text:

i) Plain Text

It is the original text or original data being sent before an encryption algorithm is applied.

ii) Cipher Text

It is the encrypted version of the plain text after an encryption algorithm is applied.



General procedure/working of encryption:

- The details/text before encryption is called plain text.
- The plain text/details are encrypted using an encryption algorithm.
- The plaint text/details are also encrypted using a key.
- The encrypted text is called cipher text.
- The key is transmitted separately from the text.
- The key is used to decrypt the cypher text after transmission.

Types of Encryptions:

1) Symmetric encryption
2) Asymmetric encryption

2.3.2 Symmetric & Asymmetric Encryption:

1) Symmetric Encryption:

- It uses the same key to encrypt and decrypt a message and so the key is referred to as either an encryption key or a decryption key depending upon its use.
- It is a security system and uses a secret key which can be a combination of characters.

How data is encrypted using symmetric encryption:

- The data before encryption is known as plain text.
- To scramble the data, an encryption key & encryption algorithm is used.
- The encryption key & algorithm are applied to plain text to convert it into cipher text.
- The data after encryption is known as cipher text which is meaningless unless the recipient also has the decryption key.
- The same key is used to encrypt and then decrypt the text.
- Encryption prevents the data from being understood by a hacker.

How encryption improves security:

- The encrypted text is meaningless.
- It needs a key to decrypt the text.

Some data is encrypted with an 8-bit key. How this encryption can be made more secure:

- It can be made more secure by increasing the length of the key such as making the key 12-bit or more etc.
- It will generate more possibilities for key and hence less chance of decryption by brute force method.

A system uses 64-bit symmetric encryption. How increase the level of security provided by the encryption:

- The length of the key can be increased by using more bits for the encryption key.
- It will generate more possibilities for key and hence less chance of decryption by brute force method.

A system uses 128-bit symmetric encryption. How the strength of encryption can be improved:

- The length of the key can be increased by using more than 128 bits for the encryption key.
- A more complex encryption algorithm can be used.
- It will generate more possibilities for key and hence less chance of decryption by brute force method.

Security Risks in Symmetric Encryption:

(i) Cracking of key:

- The modern computers can crack the encryption key in a matter of seconds.

Solution:

To overcome this issue, we now use 256-bit binary encryption keys that give 2^{256} (approximately 1.2×10^{77}) possible combinations.

(ii) Interception of Key (also known as Key Distribution Problem):

- The same key is used for encryption & decryption and so required for both sender and recipient.
- Therefore, the key has to be sent in an email or text message to the recipient which can be intercepted by, for example, a hacker which puts the security of encrypted message at risk.
- The real difficulty is keeping the encryption key a secret and so this security issue referred to as the key distribution problem is the main drawback of symmetrical encryption.

Solution:

A system based on Modulo-11 can be used, where both sender and receiver can calculate the encryption key without it actually being exchanged in any way electronically.

The following routine shows how both the sender and recipient end up with the same key without sending the actual key electronically (using Modulo-11):

- The table below is an encryption algorithm through which messages are produced in encrypted form.
- The algorithm uses an encryption key to produce a message which appears meaningless unless the same key is applied to decrypt the original message.

Stage	Sender	Recipient
1	The sender uses an encryption algorithm and chooses a value. e.g. X = 2 (this is kept secret)	The recipient uses the same algorithm and also chooses a value. e.g. Y = 4 (this is also kept secret)
2	This value of X is put into a simple algorithm: 7^x (MOD 11) *MOD gives the remainder when diving a number by 11* This gives: 7^2 (MOD 11) = 49 (MOD 11) Which gives the value: 5 (i.e. 4 remainder 5)	This value of Y is put into the same algorithm: 7^Y (MOD 11) *MOD gives the remainder when diving a number by 11* This gives: 7^4 (MOD 11) = 2401 (MOD 11) Which gives the value: 3 (i.e. 218 remainder 3)
3	The sender now sends the value just calculated (i.e. 5) to the recipient.	The recipient now sends the value just calculated (i.e. 3) to the sender.
4	This new value is put into the same algorithm – the new value replaces '7': 3^x (MOD 11) This gives: 3^2 (MOD 11) = 9 (MOD 11) Which gives the value: 9 (i.e. 0 remainder 9)	This new value is put into the same algorithm – the new value replaces '7': 5^Y (MOD 11) This gives: 5^4 (MOD 11) = 625 (MOD 11) Which gives the value: 9 (i.e. 56 remainder 9)

Drawbacks of Symmetric Key Encryption:

1. The key has to be exchanged very securely.
2. Once the key is compromised then it can be used to decrypt both sent and received messages.
3. Symmetric encryption cannot ensure non-repudiation (proof of integrity & origin of data).

Examples of Symmetric Encryption System:

1) A simple system is considered that uses a 10-digit denary encryption key and a decryption key (this gives 1 x10^{10} possible combinations). Suppose our encryption key is:

4 2 9 1 3 6 2 8 5 6 (10-digits)

which means every letter in a word is shifted across the alphabet +4, +2, +9, +1, and so on, places.

For example, a message 'COMPUTER SCIENCE IS BEST' is being sent:

Plain Text	**C**	**O**	**M**	**P**	**U**	**T**	**E**	**R**	**S**	**C**	**I**	**E**	**N**	**C**	**E**	**I**	**S**	**B**	**E**	**S**	**T**
Key Applied	4	2	9	1	3	6	2	8	5	6	4	2	9	1	3	6	2	8	5	6	4
Cipher Text	**G**	**Q**	**V**	**Q**	**X**	**Z**	**G**	**Z**	**X**	**I**	**M**	**G**	**W**	**D**	**H**	**O**	**U**	**M**	**C**	**I**	**M**

one sequence of encryption key applied

another sequence of encryption key applied

another sequence of encryption key applied

When the encryption key is applied to plain text, the following process happens:

When key is applied to plain letter 'C':

- C + shifting 4 letters = D → E → F → G
- Cipher Text of 'C' = 'G'

When key is applied to plain letter 'O':

- O + shifting 2 letters = P → Q
- Cipher Text of 'O' = 'Q'

When key is applied to plain letter 'M':

- M + shifting 9 letters = N → O → P → Q → R → S → T → U → V
- Cipher Text of 'M' = 'V'

When key is applied to plain letter 'P':

- P + shifting 1 letter = Q
- Cipher Text of 'P' = 'Q' **and so on…**

Therefore, the message is encrypted into cipher text letter by letter.

For decryption, the same key will be used to get back to original message, but the decryption process would be the reverse of the encryption:

–4 –2 –9 –1 –3 –6 –2 –8 –5 –6 (10-digits)

which means every letter in a word is shifted backward -4, -2, -9, -1, and so on.

When the decryption key is applied (same key) to cipher text, the following process happens:

When key is applied to cipher letter 'G':

- G + shifting 4 letters backwards = F → E → D → C
- Plain Text of 'G' = 'C'

When key is applied to cipher letter 'Q':

- Q + shifting 2 letters backwards = P → O
- Plain Text of 'Q' = 'O'

When key is applied to cipher letter 'V':

- V + shifting 9 letters backwards = U → T → S → R → Q → P → O → N → M
- Plain Text of 'V' = 'M'

When key is applied to letter 'Q':

- Q + shifting 1 letter backward = P
- Plain Text of 'Q' = 'P' **and so on…**

Therefore, the message is decrypted into plain text letter by letter.

2) In a simple symmetric encryption system, each letter of the alphabet is substituted with another.

The plain text message:

The quick brown fox jumps over the lazy dog.

becomes the cypher text message:

Zag towns jumpy dmh coilp mngu zag bfke qmx.

The key would be T = Z, h = a, e = g, q = t, u = o, i = w, c = n, k = s and so on…

Decoding the cypher text message: "Agbbm Pmubq"

- Hello World

Converting these words to cypher text: "Computer Science"

- Nmilozgu Pnwgyng

3) A simple symmetric encryption system is used to encrypt messages. Each letter of the alphabet is substituted by another letter.

Plain text

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Cypher text

v	p	n	a	q	b	r	u	z	s	c	o	y	k	w	f	x	i	e	m	d	j	t	l	h	g

Converting the plain text "d a t a s e c u r i t y" to cypher text:

- a v m v (data)
- e q n d i z m h (security)

a v m v e q n d i z m h (data security)

A new cypher text is created by shifting each letter of the alphabet five places to the right. Showing the new cypher text below:

Plain text

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

New cypher text

v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u

Which cypher text would be more secure?

- The first cypher is more secure.
- This is because the rest of the cypher cannot be deduced after identifying some characters as there is more random substitution and not in an alphabetic sequence.

2) Asymmetric Encryption:

It is a more secure method which overcomes security problems associated with symmetric encryption.

It makes use of two types of keys, called the public key and the private key:

- Public key is made available to everybody
- Private key is only known to the computer user.

Both types of **keys are needed to encrypt and decrypt** messages.

Public Key:

- This key is widely available and can be used to encrypt message that only the owner of private key can decrypt.

How data is encrypted using asymmetric encryption:

1. It uses a matching pair of keys (private and public).
2. A public key is made available to everyone.
3. The receiver sends their public key to the sender before a message is sent.
4. The message is encrypted by sender's computer using the public key of the receiver.
5. The encrypted message (cipher text) is then sent by sender to the receiver.
6. A private key is only known to the owner of the keys.
7. The receivers private key is used for decrypting the message after it has been received by the receiver's computer.
8. This works because the public key used to encrypt the data and the private key used to decrypt it are a matching pair generated on receivers computer.

Note:

- The public key can't be used to decrypt the message.
- The receiver can also exchange their public key with any number of people so they can receive encrypted messages (which have been encrypted using receiver's public key) and receiver can then decrypt them using matching private key.

NOTE: A number of examples have been given on the next page to better explain how asymmetric key encryption works. The standard procedure of asymmetric encryption including concepts of sender, receiver, public key, private key, encryption & decryption is same for all the examples, but they have been given for you to understand how to apply these concepts according to different scenarios asked in examination paper.

Examples of Asymmetric Encryption:

1) Wiktor is an employee of a travel agent. He uses asymmetric encryption to send confidential information to this female manager and the manager also replies confidentially. How data is encrypted using asymmetric key encryption:

- It uses different keys for encrypting (public key) and decrypting data (private key).
- When Wiktor sends a message to his manager, the message is encrypted into cipher text using his managers public key.
- When the manager receives the message, it is decrypted using her private key.
- When the manager replies, the message is encrypted using Wiktor's public key.
- When Wiktor receives the message, it is decrypted into plain text using his private key.

2) Ben wants to send a highly confidential email to Mariah so that only she can read it. How data is encrypted using asymmetric key encryption:

- It uses different keys for encrypting (public key) and decrypting data (private key).
- Ben acquires Mariah's public key.
- Ben encrypts the email using Mariah's public key.
- Ben sends the encrypted email to Mariah.
- Mariah decrypts the email using her private key.

3) Some data is being sent from one computer user to another over the internet. How data is encrypted using asymmetric key encryption:

- It uses a matching pair of keys.
- A public key is made available to everyone.
- The receivers public key is used for encrypting the message by sender before it is sent.
- A private key is only known to the owner of the keys.
- The receivers private key is used for decrypting the message after it has been received.

4) Mohammad is working away from his company's head office. He wants to send a secure message over a computer network to the head office. How data is encrypted using asymmetric key encryption:

- Two matching keys are used, one public & one private.
- Mohammad obtains the public key of head office.
- Before a message is sent, the message is encrypted by (sender's computer) using the public key of the head office.
- When the message is received at head office, it is decrypted by (receivers computer) using private key of the head office.

5) Laura wants to send an important message to her bank over the internet. How data is encrypted using asymmetric key encryption:

- Two matching keys are used, one public & one private.
- Laura obtains the public key of the bank.
- Before a message is sent, the message is encrypted by (sender's computer) using the public key of the bank.
- When the message is received at bank's computer, the message is decrypted by (receivers computer) using private key of the bank.

Benefits of Asymmetric Key Encryption:

1. It has increased message security as one key is private.
2. A private key does not need to be transmitted along with message so it cannot be intercepted by eavesdropper/hacker.
3. It allows message authentication.
4. It ensures non-repudiation (proof of integrity & origin of data).
5. It detects tampering with data.

Exam Style Questions:

Question 1:

Choose **five** correct terms from the following list to complete the spaces in the sentences below:

- cypher text
- encryption algorithm
- encryption key
- firewall
- plain text
- proxy server
- symmetric encryption

..... is a security system.

It uses the same ..... to encrypt and decrypt a message.

Before encryption, the message is called ..... .

The ..... processes the original message.

The output is known as ..... . [5]

Answer:

symmetric encryption

encryption key

plain text

encryption algorithm

cypher text [5]

Question 2:

(a) Selma has some important personal information that she needs to email to her employer.

She wants to make sure that if the personal information is intercepted, it cannot be understood.

(i) State how Selma could email her personal data more securely.

..... [1]

(ii) Describe how your chosen solution works.

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [5]

Answer:

Question	Answer	Marks
12(a)(i)	Encryption	1

Question	Answer	Marks
12(a)(ii)	Any **five** from: – Her personal details before encryption is the plain text – The plain text/her personal details is encrypted using an encryption algorithm – The plain text/her personal details is encrypted using a key – The encrypted text is cypher/cipher text – The key is transmitted **separately** (from the text) – The key is used to decrypt the cypher text (after transmission)	5

Question 3:

A company collects and stores data about its customers. The data is stored on a server in the company's office.

The data is transmitted to cloud storage to create a back-up.

The data is encrypted using symmetric encryption before it is sent to the cloud storage.

(a) Describe how the data is encrypted.

.....

.....

.....

.....

.....

.....

.....

..... [4]

Answer:

3(a)	Any **four** from: – Encryption key is used – Encryption algorithm is used – Encryption key / algorithm is applied to plain text – … to convert it into cypher text – Same key is used to encrypt and decrypt the text	**4**

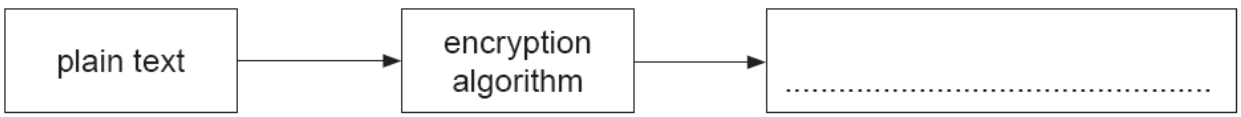
Question 4:

(b) State what is meant by symmetric encryption.

.....

..... [1]

(c) Complete the diagram:

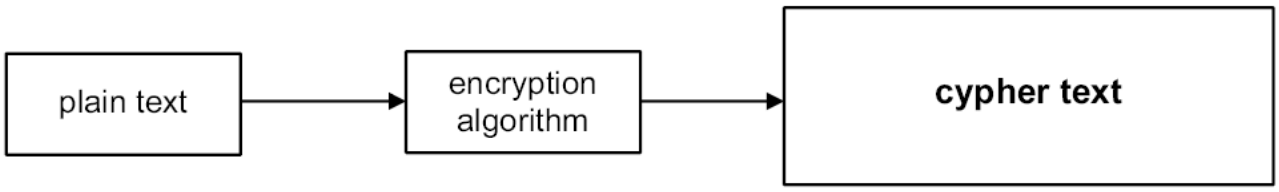


[1]

Answer:

(b) Uses the same key to encrypt and decrypt message [1]

(c) 1 mark for correct name in box



[1]

Question 5:

Complete the sentences about symmetric encryption.

Use the terms from the list.

Some of the terms in the list will **not** be used. You should only use a term once.

algorithm cipher copied delete key plain

private public standard stolen understood unreadable

The data before encryption is known as ..... text.

To scramble the data, an encryption ....., which is a type

of ....., is used.

The data after encryption is known as ..... text.

Encryption prevents the data from being ..... by a hacker. [5]

Answer:

Question	Answer	Marks
9	**One** mark for each correct term in the correct place. plain algorithm/key key/algorithm cipher understood	5

Question 6:

(c) Data transferred over a network is encrypted to improve data security.

The system uses 64-bit symmetric encryption.

(i) Explain how encryption improves data security.

.....

.....

.....

..... [2]

(ii) Explain **one** method that could be used to increase the level of security provided by the encryption.

.....

.....

.....

..... [2]

Answer:

4(c)(i)	– Encrypted text is meaningless – Need the key to decrypt the text	**2**
4(c)(ii)	– Increase length / more bits used for key … – … will generate more possibilities for key / less chance of decryption by brute force method	**2**

Question 7:

(c) Data is encrypted using 128-bit symmetric encryption before it is transmitted.

(i) Explain what is meant by encryption.

.....

.....

.....

..... [2]

(ii) State how the strength of the encryption can be improved.

Answer:

Question	Answer	Mark
2(c)(i)	Any **two** from: • Scrambles data • … making it meaningless/unintelligible • Uses an algorithm / key • Data / plain text is changed to cipher text	2
2(c)(ii)	Any **one** from: • Increase the length of the key // use more than 128 bits • Uses a more complex encryption algorithm	1

Question 8:

A simple symmetric encryption system is used to encrypt messages. Each letter of the alphabet is substituted by another letter.

Plain text

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Cypher text

v	p	n	a	q	b	r	u	z	s	c	o	y	k	w	f	x	i	e	m	d	j	t	l	h	g

(a) Convert the following plain text to cypher text.

Plain text: **d a t a s e c u r i t y**

Cypher text: .....[2]

(b) A new cypher text is created by shifting each letter of the alphabet **five** places to the right.

Show the new cypher text below.

Plain text

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

New cypher text

[2]

Answer:

4(a)	□ a v m v e q n d i z m h (2 marks, 1 for each correct word)	2
4(b)	v w x y z a b c d e f g h i j k l m n o p q r s t u **2** marks □ shift right □ all characters shifted five places	2

Question 9:

(a) Wiktor is an employee of a travel agent. He uses asymmetric encryption to send confidential information to his manager.

Fill in the spaces with an appropriate term to complete the descriptions.

Asymmetric encryption uses different …… for encrypting and decrypting data. When Wiktor sends a message to his manager, the message is encrypted into …… using his manager's …… key. When the manager receives the message, it is decrypted using her …… key. When the manager replies, the message is encrypted using Wiktor's …… key, and when Wiktor receives the message, it is decrypted into …… using his …… key. [5]

Answer:

Question	Answer	Marks
5(a)	**1 mark** per bullet point □ Keys □ Cipher text □ Manager's public and private keys in correct spaces □ Wiktor's public and private keys in correct spaces □ Plain text Asymmetric encryption uses different **keys** for encrypting and decrypting data. When Wiktor sends a message to his manager, the message is encrypted into **cipher text** using his manager's **public** key. When the manager receives the message, it is decrypted using her **private** key. When the manager replies, the message is encrypted using Wiktor's **public** key, and when Wiktor receives the message, it is decrypted into **plain text** using his **private** key.	**5**

Question 10:

Sanjeet is a member of the public, and he wants to send a private message to a government department.

(a) Explain how asymmetric encryption is used to ensure that the message remains private.

.....

.....

.....

..... [2]

(b) When the government department replies to Sanjeet, it needs to send a verified message.

Explain how asymmetric encryption can be used to ensure that it is a verified message.

.....

.....

.....

.....

.....

..... [2]

Answer:

Question	Answer	Marks
5(a)	**1 mark** per bullet point • Sanjeet's computer/software encrypts the message with the government department's public key • The government department's computer/software decrypts the message with their private key	**2**
5(b)	**1 mark** per bullet point (max 2) • The government department's computer/software creates the message digest • Sanjeet's computer/software recreates this message digest • If both copies of the message digest match the message has been verified	**2**

Question 11:

Lara wants to send an important message to her bank over the Internet.

(b) Asymmetric key cryptography is used to keep Lara's message secure during transmission over the Internet.

Describe this process of encrypting and decrypting Lara's message.

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [5]

Answer:

6(b)	Any **five** from • Two **matching** keys are used … • … one public and one private • **obtain** the public key of the bank • before the message is sent • encrypt the message in plain text using the **public key of the bank** • when the message is received at the bank's computer • decrypt the encrypted message using the **private key of the bank**	**5**

Question 12:

Ed wants to send a message securely. Before sending the message, software encrypts it using a symmetric key

(a) (i) Describe what is meant by **symmetric key encryption**.

.....

.....

.....

.....

.....

..... [2]

(ii) State **two** drawbacks of using symmetric key encryption.

.....

.....

.....

.....

.....

..... [2]

Answer:

Question	Answer	Marks
5(a)(i)	A single key is used … [1] … for both encryption and decryption [1]	**2**
5(a)(ii)	Any **two** from (max 2): Key has to be exchanged securely [1] Once compromised the key can be used to decrypt both sent and received messages [1] Cannot ensure non-repudiation (proof of integrity and origin of data) [1]	**2**