PrepWithTee

NOTES

Data Transmission

Cambridge IGCSE Computer Science (0478)

The full notes for this chapter: the topic taught from the basics, then how it is examined - question types, marking points, keywords and real past-paper questions solved - with practice to finish.

Contents

1	Data packets and packet switching	12 min
2	Serial, parallel, duplex and USB	13 min
3	Error detection: parity, checksum, echo check, ARQ, check digit	16 min
4	Encryption: symmetric and asymmetric	11 min

Each note has two parts. **Part 1** teaches the topic from the basics. **Part 2** shows how it is examined: the types of question, what the examiner gives marks for, the keywords to use, and real past-paper questions solved with the official mark scheme. The answers to every practice question are at the end of each note.

NOTE 1

Data packets and packet switching

1 In this note

SYLLABUS 2.1 TYPES AND METHODS OF DATA TRANSMISSION

- 2.1.1a Understand that data is broken down into **packets** to be transmitted.
- 2.1.1b Describe the **structure of a packet**: packet **header** (destination address, packet number, originator's address), **payload**, **trailer**.
- 2.1.1c Describe the process of **packet switching**, including the role of the **router**.

Next: Serial, parallel and duplex.

PART 1

Learn the topic

The notes: every idea from the start, with our own examples.

2 What you should already know

Everything is binary

A file, an email or a web page is just a long string of bits when it is sent.

Quick check: what is a file made of when it is sent?

A long string of bits (binary).

Networks

A network is devices connected so they can share data. The internet is a huge network of networks.

Quick check: what do we call a network of networks?

The internet.

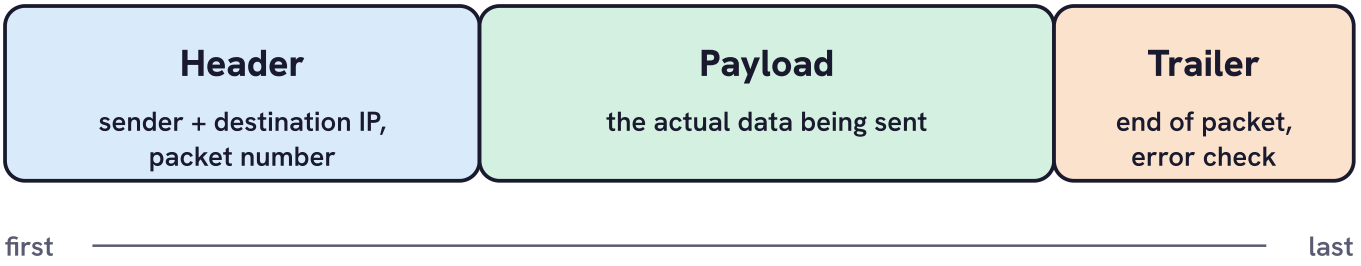
3 Why data is split into packets

When a file is sent across a network it is not sent in one go. It is **broken down into small units** called **packets**. Each packet is sent **independently** and the file is put back together at the other end.

Why? A small packet is quick to send. If one packet is lost or damaged, only that packet has to be sent again, not the whole file. And many people can share the same network, because packets from different users take turns on the cables.

4 The structure of a packet

Every packet has **three sections**: a **header**, a **payload** and a **trailer**.



A packet: the header goes first, then the data (payload), then the trailer.

Section	What it holds
Header	the **destination address** (IP address of the receiver), the **originator's address** (IP address of the sender) and the **packet number** (so the packets can be put back in order). It can also give the size of the packet and the total number of packets.
Payload	the **actual data** being sent: one small piece of the file
Trailer	data that shows the **end of the packet**, and **error checking** data (e.g. a checksum value)

> Memory hook: the **header** is like the address and number written on an envelope, the **payload** is the letter inside, the **trailer** says "end of letter" and how to check it arrived complete.

TRY IT YOURSELF

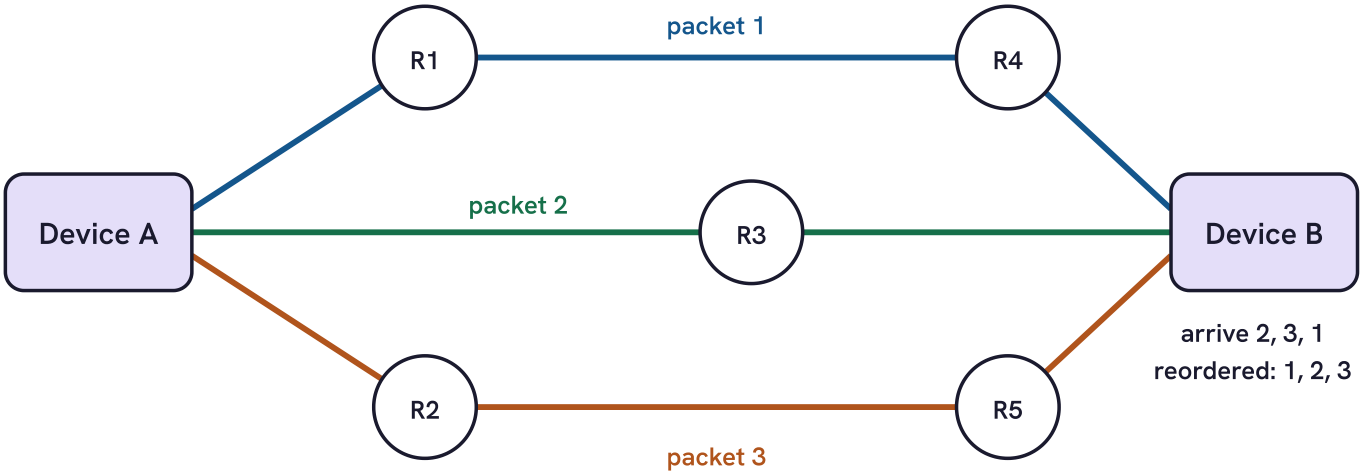
1. Which section of a packet holds the packet number?
2. Which section holds the actual data being sent?
3. Give one item of data stored in the trailer.

5 Packet switching

Packet switching is the method used to send the packets across a network such as the internet. A device called a **router** sits at each junction of the network and decides where each packet goes next.

GENERAL METHOD **How packet switching works**

1. The data is **broken down into packets**.
2. Each packet is given a header with the destination address and its **packet number**.
3. Each packet is sent **independently**: it **could take a different route** across the network.
4. At each **router**, the router reads the **destination address** in the header and sends the packet on towards its destination, choosing the **shortest / fastest available route** at that moment.
5. Packets may **arrive out of order** (some routes are slower or busier).
6. When the **last packet** has arrived, the packets are **reordered** using their packet numbers.
7. If a packet is **missing or corrupted**, it is **requested again**.



Three packets of one file take three different routes through the routers, arrive in the order 2, 3, 1 and are put back in order at B.

Advantages of packet switching	Disadvantages
packets can **avoid busy or broken routes**, so data still gets through	packets can **arrive out of order** and must be reordered
only a **lost / damaged packet is resent**, not the whole file	packets can be **lost** and need resending, which causes delay
many users can **share the network** at the same time	the receiver must wait for every packet before the file is complete

TRY IT YOURSELF

1. Name the device that controls the route each packet takes.
2. Why might packets arrive in a different order from the order they were sent?

6 Summary

- Data is broken down into packets; each packet is sent independently.
- Header: destination address, originator's address, packet number. Payload: the data. Trailer: end of packet + error checking.
- Packet switching: each packet may take a different route; routers read the destination address and send it on by the best route.
- Packets can arrive out of order; they are reordered (packet numbers) once the last one arrives; missing ones are requested again.

IF YOU SEE …

"describe the structure of a packet"	→ three sections · header (with 2 examples) · payload (the data) · trailer (end + error check)
"explain how packet switching works"	→ split into packets · different routes · router · out of order · reordered · resent
"purpose of a router"	→ reads destination address · sends packet towards destination · chooses the route

PART 2

How it is examined

Question types, what the examiner gives marks for, and real past-paper questions solved.

7 Ways they test it

TYPE 1 **Header items**

> *"Identify two items of data contained in a packet header" [2]*

Spot it "header".

1. Destination IP address · originator's (sender's) IP address · packet number. Not "the data" (that is the payload).

TYPE 2 **Structure**

> *"Describe the structure of a data packet" [3-6]; a labelled diagram to complete*

Spot it "structure", "sections".

1. Name all three sections in order AND say what each holds: one mark per name, one per example.

TYPE 3 **Process**

> *"Explain how the file is transmitted using packet switching" [5]; "complete and annotate the diagram" [4]*

Spot it "packet switching", "routers".

1. Write the method steps in order: split, different routes, router, out of order, reordered, resent.

TYPE 4 **Router**

> *"Give the purpose of a router in packet switching" [1]; "identify the component that ..." [1]*

Spot it "controls the route".

1. Router: reads the destination address and sends the packet towards its destination by the best route.

TYPE 5 **Cloze**

> *"Complete the statements ... use the terms from the list" [4]*

Spot it a word list.

1. Each gap uses a keyword from the notes: header, destination address, routers, last.

8 What the examiner looks for

"Describe the structure of a packet of data" [4]

Marking points (one mark each, up to the marks shown)

- The data packet has three sections
- It has a packet header ...
- ... that contains data such as the destination address
- It has a payload ...
- ... that contains the main data
- It has a trailer ...
- ... that contains data such as the error detection method used

KEYWORDS **header** **payload** **trailer** **destination address** **packet number**

"Explain how the file is transmitted using packet switching" [5]

Marking points (one mark each, up to the marks shown)

- Data is broken / split / divided into packets
- Each packet (could) take a different route
- A router controls the route / path a packet takes ...
- ... selecting the shortest / fastest available route
- Packets may arrive out of order
- Once the last packet has arrived, packets are reordered
- If a packet is missing / corrupted, it is requested again

KEYWORDS **packets** **different route** **router** **out of order** **reordered**

Wording trap · Packet header

THE QUESTION **0478/11/M/J/25 Q4** ↗ Paper 1 · Computer systems **1 mark**

Which item would NOT be included in a packet's header? A destination address · B originator's address · C packet number · D payload

✓ CREDITED

- D, payload: the payload is a separate section, the data itself

✗ NOT CREDITED

- A, B or C: these three are exactly what the header holds

WHY

The header describes the packet; the payload IS the data.

From: 0478/11/M/J/25 Q4(c)(i) mark scheme

9 Past-paper questions, solved

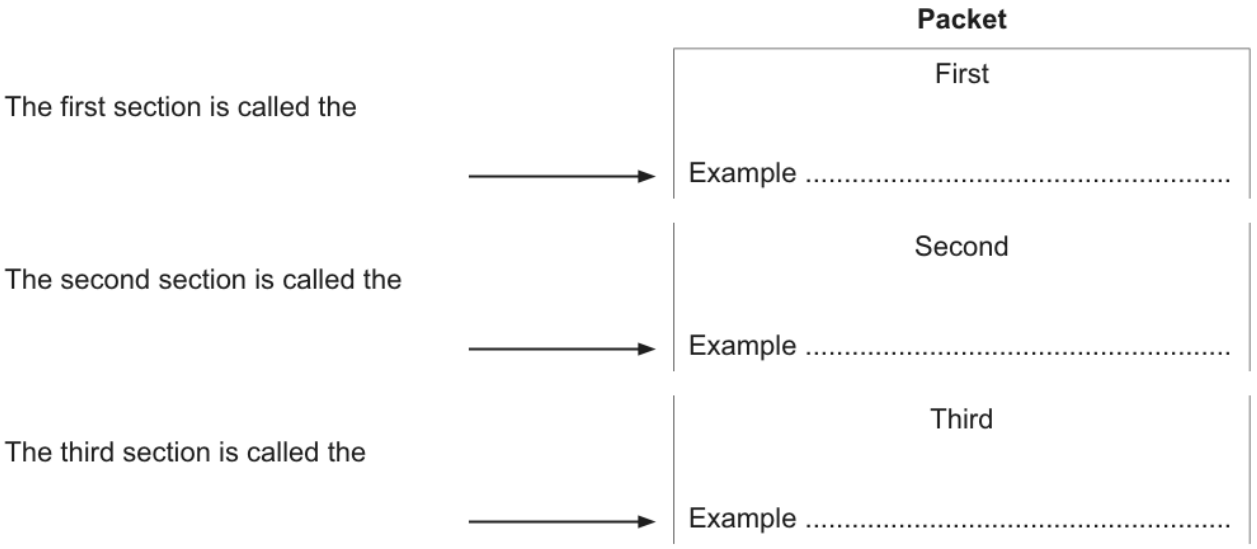
0478/13/O/N/25 Q3 ↗ Paper 1 · Computer systems **6 marks** ⤢ Full size

3 Data is split into packets before it is transmitted across a network.

(a) The diagram shows a packet with **three** sections.

Complete the diagram by writing the name of each section of the packet.

Write an example in each section of what would be stored in that part of the packet.



[6]

Swipe sideways to read the whole question

How to start Three sections, three examples: one mark each. Write them in order: first, second, third.

▼ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

First section: the **header**. Example: the destination IP address (or packet number, or sender's IP address).

Second section: the **payload**. Example: the data itself.

Third section: the **trailer**. Example: error checking data (or end of packet notification).

PART	ANSWER / WORKING	MARKS	GUIDANCE
3(a)	Header · e.g. originator's / destination (IP) address, packet number	B2	
	Payload · the data itself	B2	
	Trailer · e.g. end of packet notification, error checking data	B2	

Total: 6 marks

0478/11/M/J/23 Q2 ↗ Paper 1 · Computer systems **7 marks** ⤢ Full size

2 A student has a sound file that is too large to be stored on their external secondary storage device. The student compresses the sound file to make the file size smaller.

The compression method used reduces the sample rate and the sample resolution of the sound file.

(c) The student sends the sound file to a friend. The file is transmitted across a network that uses packet switching.

(i) Identify **two** pieces of data that would be included in the header of each packet.

[2]

(ii) Explain how the file is transmitted using packet switching.

..... [5]

Swipe sideways to read the whole question

How to start (i) is two of the three header items. (ii) is the seven-step method: aim for five clear points.

▼ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

(c)(i) The destination IP address. The packet number.

(c)(ii) The file is broken down into packets. Each packet can take a different route across the network. Routers control the route each packet takes, choosing the fastest available route. The packets may arrive out of order, so once the last packet has arrived they are reordered using the packet numbers. If a packet is missing or corrupted it is requested again.

PART	ANSWER / WORKING	MARKS	GUIDANCE
2(c)(i)	Any two: destination (IP) address · packet number · originator's (IP) address	B2	
2(c)(ii)	Any five: split into packets · different routes · router controls the route · … shortest / fastest route · may arrive out of order · reordered once the last arrives · missing / corrupted packet requested again	B5	

Total: 7 marks

0478/11/O/N/23 Q7 ↗ Paper 1 · Computer systems **4 marks** ⤢ Full size

7 Complete the statements about data packets and packet switching.

Use the terms from the list.

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

destination address first footer header

last main data packets payload

routers servers trailer

Data is broken down into packets. A data packet has a packet ..... that contains the packet number and the ..... .

Each packet could take a different path from the sender to the receiver; this is controlled by ..... .

Packets may arrive out of order. Once the ..... packet has arrived, the packets are reordered.

[4]

Swipe sideways to read the whole question

How to start Read the whole paragraph first. Each gap matches one keyword from the notes; not every word in the list is used.

▼ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

header · destination address · routers · last

(A packet has a packet **header** that contains the packet number and the **destination address**. The path is controlled by **routers**. When the **last** packet arrives, the packets are reordered.)

PART	ANSWER / WORKING	MARKS	GUIDANCE
7	header · destination address · routers · last, one mark each in the correct order	B4	

Total: 4 marks

10 Common mistakes

✗ "The header contains the data"

The header only describes the packet.

✓ "The payload contains the data"

✗ "All packets take the same route"

✓ "Each packet can take a different route"

✗ "The router puts the packets back in order"

The router only sends each packet on.

✓ "The receiving device reorders the packets"

✗ "Address" on its own

Say which address.

✓ "Destination IP address" or "sender's IP address"

11 Practice

Practice: easy, medium, hard

1. What is the name given to the small units that data is broken into for transmission?
2. Name the three sections of a packet, in order.
3. Give the purpose of the packet number.
1. Give two items of data stored in a packet header.
2. Explain why packets may need to be reordered when they arrive. [2]
3. Describe the role of a router in packet switching.
1. A video is sent across the internet using packet switching. Explain how the video is transmitted. [5]
2. Give one benefit and one drawback of packet switching.

12 Can I do this?

0 / 3 ticked

- [ ] I can explain why data is split into packets.
- [ ] I can name the three sections of a packet and say what each holds.
- [ ] I can explain packet switching in order, including the router.

Anything unticked: revise that section first (each line links to it). All ticked: take the quiz.

Answers

Answers to the "Try it yourself" and practice questions on this page. Try every question first.

Try it yourself 1

1.

ANSWER The header

2.

ANSWER The payload

3.

ANSWER End of packet notification / error checking data such as a checksum

Try it yourself 2

1.

ANSWER Router

2.

ANSWER

Each packet can take a different route; some routes are longer or busier, so some packets take longer

Practice: easy, medium, hard

Easy 1.

ANSWER Packets

Easy 2.

ANSWER Header, payload, trailer

Easy 3.

ANSWER So the packets can be put back in the correct order when they arrive

Medium 1.

ANSWER Two of: destination IP address, originator's IP address, packet number

Medium 2.

ANSWER

Each packet can take a different route; some take longer, so they arrive in the wrong order

Medium 3.

ANSWER

Reads the destination address in the header and sends the packet towards its destination by the best available route

Hard 1.

ANSWER

Split into packets with header (destination address, packet number); each packet sent independently, may take a different route; routers read the destination address and choose the fastest route; packets arrive out of order; reordered when the last arrives; missing / corrupted packets requested again

PART	ANSWER / WORKING	MARKS	GUIDANCE
	split into packets	B1	
	different routes	B1	
	router chooses route	B1	
	out of order → reordered when last arrives	B1	
	missing packets requested again	B1	
		Total: 5 marks	

Hard 2.

ANSWER

Benefit: packets avoid busy / broken routes, only lost packets resent. Drawback: packets arrive out of order / can be lost, causing delay

NOTE 2

Serial, parallel, duplex and USB

1 In this note

SYLLABUS 2.1 TYPES AND METHODS OF DATA TRANSMISSION

- 2.1.2a Describe **serial** and **parallel** transmission, and **simplex**, **half-duplex** and **full-duplex** transmission.
- 2.1.2b Explain the **suitability** of each method for a given situation, with **advantages and disadvantages**.
- 2.1.3 Understand the **universal serial bus (USB)** interface and how it is used to transmit data.

Before this: Packets and packet switching. Next: Error detection.

PART 1

Learn the topic

The notes: every idea from the start, with our own examples.

2 What you should already know

Bits

All data is sent as bits (1s and 0s). Eight bits make a byte.

Quick check: how many bits in a byte?

8.

Interference

Electrical signals in wires can be disturbed by other signals nearby. This can change a 1 into a 0, or a 0 into a 1.

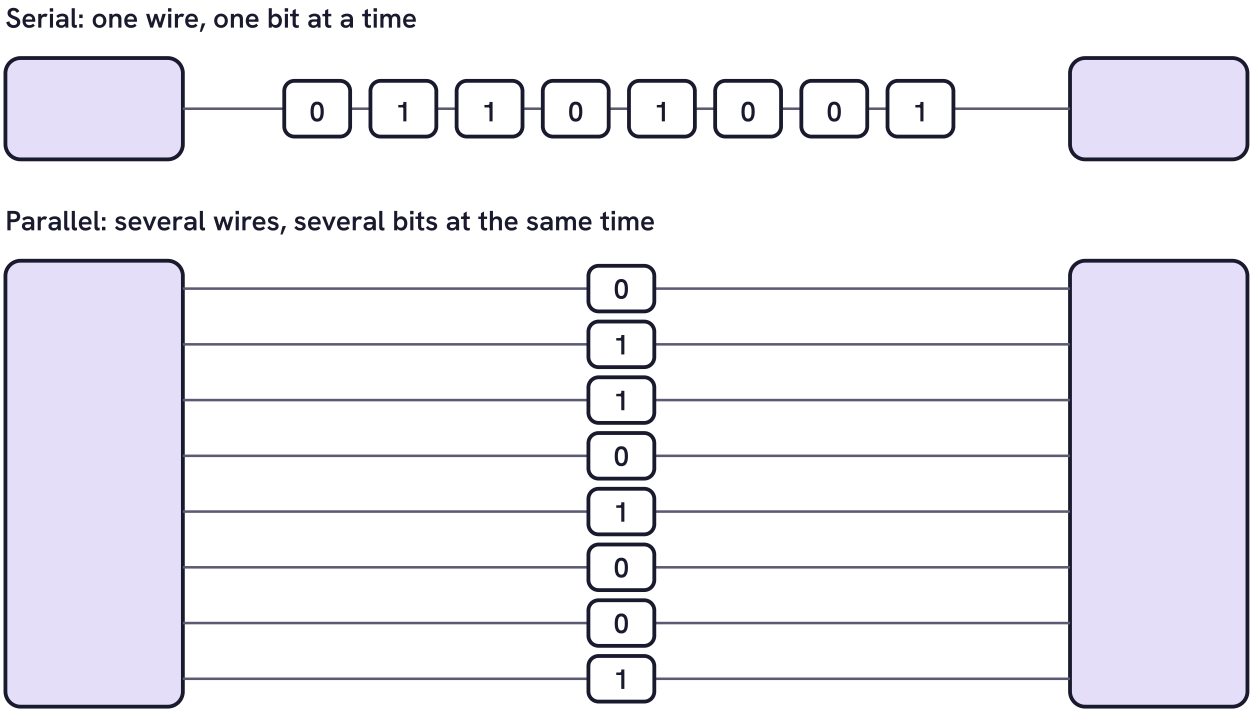
Quick check: what can interference do to a bit?

Change it (flip a 1 to a 0 or a 0 to a 1).

3 Serial and parallel

Every method is described in two ways: **how many wires** are used (serial or parallel) and **which directions** the data can go (simplex, half-duplex or full-duplex). An answer always needs both,

e.g. "serial half-duplex".

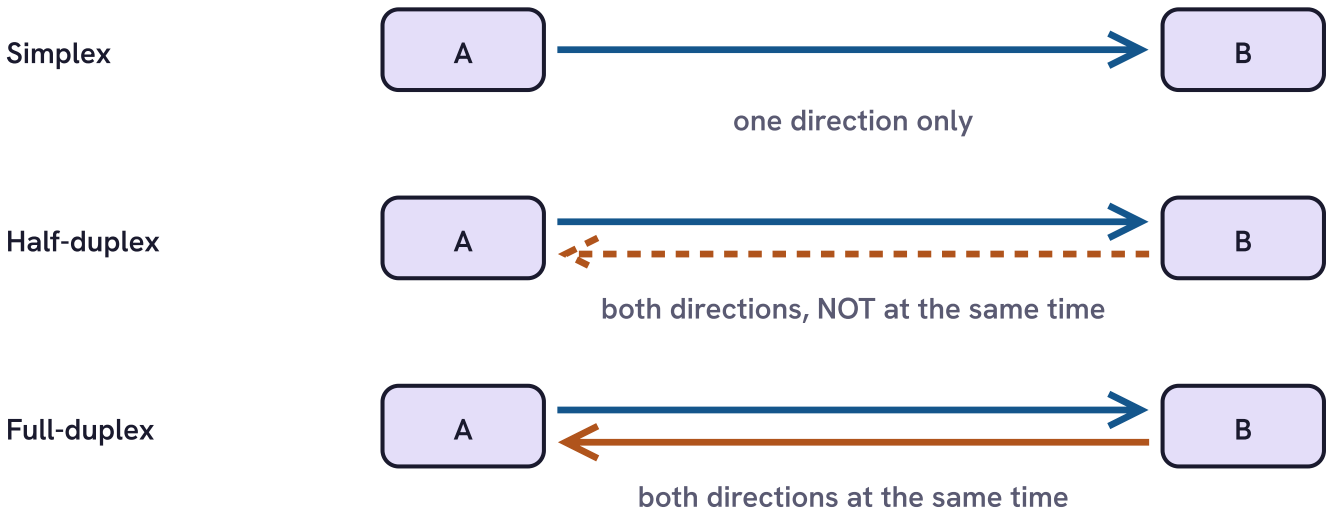


Serial sends the 8 bits one after another down one wire. Parallel sends 8 bits at once, one on each wire.

	Serial	Parallel
How	data is sent **one bit at a time** down a **single wire**	**several bits at the same time** down **several wires**
Speed	slower	**faster** (several bits at once)
Order of bits	bits **arrive in order**: they **cannot be skewed**	bits can arrive at slightly different times: **skewing**
Errors	**less interference / crosstalk**, so fewer errors	wires next to each other cause **crosstalk**, so more errors
Distance	reliable over **long distances**	only reliable over **short distances** (skewing gets worse with length)
Cost	cheaper: one wire	more expensive: many wires
Typical use	USB, networks, long cables	inside a computer (e.g. buses), very short cables

Skewing: the bits sent at the same time down parallel wires arrive at slightly different times, so they can be read out of order. **Crosstalk**: interference between wires that are next to each other.

4 Simplex, half-duplex and full-duplex



The three directions of transmission.

Method	What happens	Example
Simplex	data is sent in **one direction only**	computer to monitor; microphone to speakers
Half-duplex	data is sent in **both directions**, but **only one direction at a time**	walkie-talkie; a printer cable that also sends back "out of paper"
Full-duplex	data is sent in **both directions** **at the same time**	phone call; a network connection with upload and download together

TRY IT YOURSELF

1. Data is sent down one wire, one bit at a time, in both directions but not at the same time. Name the method.
2. Which method is fastest over a 30 cm cable: serial simplex or parallel simplex?
3. Give one reason serial is used for long distances.

5 Choosing a method for a situation

GENERAL METHOD **Choose and justify a method**

1. **Distance**: more than a few metres → **serial** (no skewing, less interference). Very short and speed matters → **parallel**.
2. **Speed / amount of data**: small amounts of data → serial is **fast enough**. Lots of data quickly over a short distance → parallel.
3. **Direction**: does data only go one way? → **simplex**. Does a reply come back but not at the same time? → **half-duplex**. Do both sides send at once? → **full-duplex**.
4. Write each reason as **point + because**: "serial, because the data travels a long distance and the bits will not be skewed".

EXAMPLE **A school's printer is in the next room. The computer sends documents; the printer sends back "paper jam" messages, but never while it is receiving. Choose a method.**

Two decisions: wires, then directions.

Distance: the next room, several metres → serial (bits not skewed, less interference).

Directions: both ways, but not at the same time → half-duplex.

ANSWER **Serial half-duplex**

6 The universal serial bus (USB)

USB is a standard way to connect devices (mouse, keyboard, printer, memory stick, phone) to a computer. It uses **serial** transmission: data is sent **one bit at a time** down a **single wire**. Newer versions can send in both directions.

Benefits of USB	Drawbacks of USB
it is a **universal standard**, so most devices and computers have it	**maximum cable length** is short (about 5 m)
the cable **can only be inserted one way** / cannot be plugged in wrongly	slower than some other connections (e.g. a parallel connection)
the device is **automatically detected** and the **driver installed automatically**	older versions may be slow for big transfers
it can **power the device** (and charge it)	
backwards compatible with older USB versions; supports different speeds	
serial, so **less chance of skewing / errors**	

TRY IT YOURSELF

1. Is USB serial or parallel?
2. Give two benefits of connecting a mouse by USB.

7 Summary

- Serial: one bit at a time, one wire; in order, less interference, long distances, slower.
- Parallel: several bits at the same time, several wires; faster, but skewing and crosstalk, short distances only.
- Simplex: one direction. Half-duplex: both directions, one at a time. Full-duplex: both directions at the same time.
- Choose by distance, speed needed and direction; justify each choice with a reason.
- USB = universal serial bus: serial, universal, auto-detected, powers the device, one-way plug; short cable.

IF YOU SEE …

"describe serial half-duplex"	→ one bit at a time · single wire · both directions · not at the same time
"explain why serial is suitable"	→ long distance · bits not skewed · less interference · speed adequate
"benefits of USB"	→ universal · auto-detected / driver · powers device · cannot insert wrongly · backwards compatible

PART 2

How it is examined

Question types, what the examiner gives marks for, and real past-paper questions solved.

8 Ways they test it

TYPE 1 Describe a method

> *"Explain how data is transmitted using serial full-duplex" [4]*

Spot it a method name with two words.

1. Two marks for the wire part (one bit at a time / single wire) and two for the direction part (both directions / at the same time).

TYPE 2 Name from a description

> *a table of descriptions to complete [4]; "circle the two methods" [2]*

Spot it "identify", "circle".

1. Read each description twice: once for the wires, once for the directions.

TYPE 3 Choose and justify

> *"Identify the most appropriate method. Explain your choice" [5]*

Spot it a scenario: distance, who sends what.

1. One mark per word of the method; then reasons tied to the scenario (distance, direction, speed).

TYPE 4 Benefits / drawbacks

> *"Give two drawbacks of using parallel full-duplex" [2]*

Spot it "benefit", "drawback".

1. Use the comparison table: skewing, crosstalk, collisions, distance, speed.

TYPE 5 **USB**

> *"Explain how data is sent using USB" [2]; "give two benefits" [2]*

Spot it "USB".

1. How: one bit at a time, single wire. Benefits from the USB table.

9 What the examiner looks for

"Explain how data is transmitted using serial full-duplex / parallel half-duplex" [4]

Marking points (one mark each, up to the marks shown)

- Serial: data is sent one bit at a time … down a single wire
- Parallel: data is sent multiple bits at the same time … down multiple wires
- Full-duplex: data can be sent in both directions … at the same time
- Half-duplex: data can be sent in both directions … but not at the same time
- Simplex: data is sent in one direction only

KEYWORDS **one bit at a time** **single wire** **multiple wires** **both directions** **at the same time**

"Explain why serial is the most appropriate method" [3]

Marking points (one mark each, up to the marks shown)

- The data may travel a long distance … serial is more reliable over long distances
- Bits are sent / arrive in order … so the data will not be skewed
- Less interference / crosstalk (single wire) … so fewer errors
- The data does not need to be sent quickly … only small amounts of data, so serial speed is adequate

KEYWORDS **long distance** **skewed** **interference** **crosstalk** **adequate speed**

TOO VAGUE "it is faster" (serial is not faster); "it is safer" (say why: fewer errors)

Wording trap · Choosing a method

THE QUESTION **0478/11/M/J/25 Q4** ↗ Paper 1 · Computer systems — **1 mark**

Give one improvement that would be made to the data transmission if parallel transmission is used instead of serial transmission.

✓ CREDITED

- The data may be transmitted faster

✗ NOT CREDITED

- it is more secure
- fewer errors
- it can go further

WHY

Parallel's only advantage is speed. It has MORE errors and works over SHORTER distances.

From: 0478/11/M/J/25 Q4(a)(ii) mark scheme

10 Past-paper questions, solved

0478/12/O/N/23 Q6 ↗ Paper 1 · Computer systems **4 marks** ⤢ Full size

6 The table contains descriptions about data transmission methods.

Complete the table by identifying which data transmission methods are described.

Data transmission method	Description
.....	Data is transmitted down a single wire, one bit at a time, in one direction only.
.....	Data is transmitted down multiple wires, multiple bits at a time, in both directions, but only one direction at a time.
.....	Data is transmitted down a single wire, one bit at a time, in both directions at the same time.
.....	Data is transmitted down multiple wires, multiple bits at a time, in one direction only.

Swipe sideways to read the whole question

How to start Each description has two parts. Single wire, one bit = serial; multiple wires = parallel. Then the direction words.

▼ Show a full-mark answer and the mark scheme · official marking

WHAT TO WRITE

serial simplex · parallel half-duplex · serial full-duplex · parallel simplex

PART	ANSWER / WORKING	MARKS	GUIDANCE
6	serial simplex · parallel half-duplex · serial full-duplex · parallel simplex (one mark each)	B4	

Total: 4 marks

0478/11/O/N/25 Q7 ↗ Paper 1 · Computer systems — **5 marks** — ⤢ Full size

7 A theatre has a microphone on stage that is connected by cables to several speakers around the theatre. A person speaks into the microphone and their voice is output from the speakers.

Identify the most appropriate data transmission method for this purpose. Explain your choice.

Data transmission method .....

Explanation .....

[5]

Swipe sideways to read the whole question

How to start Two marks for the method (one for each word), three for reasons. Look for distance (around the theatre) and direction (sound only goes from microphone to speakers).

▼ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

Method: serial simplex.

Explanation: Serial, because the cables run a long distance around the theatre, and the bits are sent one at a time down one wire, so they will not be skewed and there is less chance of error. Simplex, because the data only needs to go in one direction, from the microphone to the speakers; nothing is sent back.

PART	ANSWER / WORKING	MARKS	GUIDANCE
7	Serial · Simplex	B2	
	Any three: long distance · one wire / bits in order · less chance of skewing / error · speed adequate · only one direction needed · nothing sent back from speakers to microphone	B3	

Total: 5 marks

4 A company decides to create a network for its devices.

All the company devices are within a single room.

The employees will need to use their devices to send data to each other and share files.

The company decides to send data across the network using packet switching.

(b) The company decides to use parallel full-duplex data transmission to send the data across the network.

(i) Explain the reasons why the company have chosen this method of data transmission.

..... [4]

(ii) Give **two** drawbacks of the company using this method of data transmission.

[2]

(iii) Give **one** other method of data transmission the company could have chosen.

..... [1]

Swipe sideways to read the whole question

How to start (i) Give a point AND its link to the scenario (single room, sending to each other). (ii) is the parallel and full-duplex drawbacks. (iii) any other method.

▼ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

(b)(i) Parallel sends multiple bits at the same time down multiple wires, so the data is transmitted quickly. The data does not need to travel a long distance, as the devices are all in a single room. Full-duplex sends data in both directions at the same time, so employees can send data to each other with no delay.

(b)(ii) More interference / crosstalk because of the multiple wires. Bits may be skewed and arrive out of order.

(b)(iii) Serial full-duplex.

PART	ANSWER / WORKING	MARKS	GUIDANCE
4(b)(i)	Any four: multiple bits / multiple wires · … fast · short distance · … single room · both directions at the same time · … no delay	**B4**	
4(b)(ii)	Any two: interference / crosstalk · skewed / out of order · data collisions · more errors	**B2**	
4(b)(iii)	Any other combination, e.g. serial full-duplex	**B1**	

Total: 7 marks

0478/12/O/N/25 Q5 ↗ Paper 1 · Computer systems **5 marks** ⤢ Full size

5 A computer system has a mouse.

An interrupt is sent to the CPU every time a button on the mouse is clicked.

(c) The mouse is connected using a universal serial bus (USB) connection.

(i) Explain how data is sent using the USB connection.

..... [2]

(ii) Give **two** benefits of using a USB connection for this purpose.

[2]

(iii) Give **one** drawback of using a USB connection for this purpose.

..... [1]

Swipe sideways to read the whole question

How to start USB is serial: that gives (i). For (ii) and (iii) use the USB benefits / drawbacks, linked to a mouse.

▼ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

(c)(i) The data is sent one bit at a time down a single wire.

(c)(ii) The mouse is powered by the computer through the cable. The mouse is automatically detected and its driver is installed automatically.

(c)(iii) The wire may get in the way and limit the movement of the mouse.

PART	ANSWER / WORKING	MARKS	GUIDANCE
5(c)(i)	one bit at a time · single wire	B2	
5(c)(ii)	Any two: powered by the device · universal · backward compatible · less skewing / errors · different speeds · cannot be inserted incorrectly · automatically detected / driver installed	B2	
5(c)(iii)	slower than parallel // wire gets in the way / limits movement	B1	

Total: 5 marks

11 Common mistakes

✗ "Serial is faster"

✓ "Parallel is faster; serial is more reliable over distance"

✗ Naming only half a method: "half-duplex"

✓ "Serial half-duplex"

Questions about a method want both parts.

✗ "Half-duplex sends one way"

✓ "Both ways, but only one direction at a time"

One way only is simplex.

✗ "Serial is more secure"

✓ "Fewer errors, because bits are not skewed and there is less interference"

Security is not the point.

12 Practice

Practice: easy, medium, hard

1. Describe serial transmission.
2. Name the method: both directions at the same time.
3. What does USB stand for?
1. Give two drawbacks of parallel transmission.
2. A keyboard sends key presses to a computer; nothing is sent back. Which direction method is this?
3. Explain how data is sent using parallel half-duplex. [4]
1. Two computers 40 m apart exchange files, both sending and receiving at once. Identify the most appropriate method and justify it. [5]
2. Give one drawback of a USB connection for an external hard drive.

13 Can I do this?

0 / 4 ticked

- [ ] I can describe serial and parallel and compare them.
- [ ] I can describe simplex, half-duplex and full-duplex.
- [ ] I can choose a method for a scenario and justify both parts.
- [ ] I can explain how USB sends data and give its benefits and drawbacks.

Anything unticked: revise that section first (each line links to it). All ticked: take the quiz.

Answers

Answers to the "Try it yourself" and practice questions on this page. Try every question first.

Try it yourself 1

1.

ANSWER Serial half-duplex

2.

ANSWER Parallel simplex

3.

ANSWER Bits are not skewed / less interference, so fewer errors

Try it yourself 2

1.

ANSWER Serial

2.

ANSWER

Two of: powers the mouse, automatically detected / driver installed, universal, cannot be inserted wrongly

Practice: easy, medium, hard

Easy 1.

ANSWER Data is sent one bit at a time down a single wire

Easy 2.

ANSWER Full-duplex

Easy 3.

ANSWER Universal serial bus

Medium 1.

ANSWER

Skewing (bits arrive out of order); crosstalk / interference; only short distances; more expensive

Medium 2.

ANSWER **Simplex**

Medium 3.

ANSWER

Multiple bits at the same time · down multiple wires · in both directions · but not at the same time

Hard 1.

ANSWER

Serial full-duplex. Serial: long distance (40 m), bits not skewed, less interference so fewer errors. Full-duplex: both computers need to send and receive at the same time, so no waiting.

PART	ANSWER / WORKING	MARKS	GUIDANCE
	serial	B1	
	full-duplex	B1	
	long distance / not skewed / fewer errors (max 2)	B2	
	both directions at the same time	B1	
			Total: 5 marks

Hard 2.

ANSWER **Maximum cable length is short / slower than some other connections**

NOTE 3

Error detection: parity, checksum, echo check, ARQ, check digit

1 In this note

SYLLABUS 2.2 METHODS OF ERROR DETECTION

- 2.2.1 Understand the **need to check for errors** after transmission and **how errors can occur**.
- 2.2.2 Describe **parity check** (odd / even, parity byte, parity block), **checksum** and **echo check**.
- 2.2.3 Describe how a **check digit** detects errors in **data entry**.
- 2.2.4 Describe how an **automatic repeat query (ARQ)** checks that data is received without error.

Before this: Serial, parallel and duplex. Next: Encryption.

PART 1

Learn the topic

The notes: every idea from the start, with our own examples.

2 What you should already know

Odd and even

Count the 1s in a byte: 3 ones is odd, 4 ones is even.

Quick check: is 1011 0010 odd or even?

Four 1s: even.

Packets

Data is sent in packets, each with a header, payload and trailer.

Quick check: which section holds error checking data?

The trailer.

3 Why errors happen and why we check

Data can be correct when it leaves the sender but wrong when it arrives. During transmission, data can be **lost**, **gained** (extra bits added) or **changed** (a 1 becomes a 0). Causes:

Cause	What happens
Interference	electrical noise from other devices disturbs the signal and flips bits
Crosstalk	signals in wires next to each other interfere (worse in parallel cables)
Skewing	bits sent together in parallel arrive at different times and are read in the wrong order
Data collisions / lost packets	two signals meet, or a packet is dropped or times out on its way

A file with even one wrong bit can be useless (a program that crashes, a wrong bank amount). So the receiver checks the data, and asks for it again if it is wrong.

4 Parity check

Sender and receiver agree on **odd parity** or **even parity**. Each byte has 7 data bits and one **parity bit** (usually the leftmost bit). The parity bit is set so the **number of 1s in the byte** is odd (odd parity) or even (even parity).

GENERAL METHOD **Parity byte check**

1. Before sending, **count the 1s** in the 7 data bits.
2. Set the **parity bit** to 0 or 1 so the byte's total number of 1s matches the agreed parity (odd or even).
3. Send the byte.
4. After transmission, the receiver **counts the 1s** in each byte again.
5. If the count **does not match the agreed parity**, an **error is detected** and the data is sent again.

EXAMPLE **Add the parity bit to the data 110 1001 for even parity, then for odd parity.**

Count the 1s in the 7 data bits.

1101001 has four 1s: already even.

Even parity: parity bit 0 → 0110 1001 (four 1s).

Odd parity: parity bit 1 → 1110 1001 (five 1s).

ANSWER **even: 0, odd: 1**

✗ COMMON MISTAKE

A parity check **cannot find every error**. If **two bits** change (or two bits swap places, a **transposition**), the number of 1s is still odd / even, so the error is **not detected**. A parity byte check also cannot say **which** bit is wrong.

Parity block check

A **parity block** check sends several bytes together, each with a parity bit, plus an extra **parity byte** at the end. Each bit of the parity byte makes its **column** match the parity. The receiver checks every row and every column: the wrong bit is where the **bad row and bad column cross**, so it can be **located and corrected**.

Four bytes sent with even parity:

	Parity bit	bit 1	bit 2	bit 3	bit 4	bit 5	bit 6	bit 7	1s
Byte 1	0	1	0	1	1	0	0	1	4
Byte 2	0	0	1	1	0	1	0	1	4
Byte 3	0	1	1	0	0	0	1	1	4
Byte 4	1	0	0	0	1	1	1	0	4
Parity byte	1	0	0	0	0	0	0	1	2

After transmission one bit has changed:

	Parity bit	bit 1	bit 2	bit 3	bit 4	bit 5	bit 6	bit 7	1s
Byte 1	0	1	0	1	1	0	0	1	4
Byte 2	0	0	1	1	0	1	0	1	4
Byte 3	0	1	1	0	0	1	1	1	5
Byte 4	1	0	0	0	1	1	1	0	4
Parity byte	1	0	0	0	0	0	0	1	2

Byte 3 now has 5 ones (odd), and column bit 5 has an odd number of 1s. The error is the bit where byte 3 meets bit 5, so the receiver can flip it back.

TRY IT YOURSELF

1. Give the even parity bit for the data 011 0001.
2. Give the odd parity bit for the data 011 0001.
3. Two bits in a byte are flipped. Will a parity byte check detect it? Why?

5 Checksum

GENERAL METHOD **Checksum**

1. Before sending, a **checksum value is calculated** from the data using an **algorithm** (e.g. adding up the byte values).
2. The checksum is **sent with the data** (in the packet trailer).
3. The receiver **recalculates** the checksum from the data it received, using the **same algorithm**.
4. The two checksums are **compared**: if they are **different, an error is detected** and the data is requested again; if they match, no error.

EXAMPLE **Bytes with the values 200, 150, 90 and 37 are sent. The checksum algorithm adds the values and keeps the remainder after dividing by 256. Find the checksum.**

Add, then find the remainder after 256.

$200 + 150 + 90 + 37 = 477$

$477 - 256 = 221$

ANSWER **checksum = 221**

6 Echo check

GENERAL METHOD **Echo check**

1. The data is sent to the receiver.
2. The receiver sends a **copy of the data it received back** to the sender.
3. The sender **compares the original data with the copy**.
4. If they **do not match**, an error has occurred and the data is sent again.

✗ COMMON MISTAKE

Drawback: if the copy does not match, it is not known whether the error happened on the way there or on the way back. It also doubles the amount of data sent.

7 Automatic repeat query (ARQ)

An **ARQ** (automatic repeat query / request) uses **acknowledgements** and a **timeout** so that each packet is received without error. The receiver checks each packet with an error detection method (e.g. a checksum).

GENERAL METHOD **ARQ with a positive acknowledgement**

1. The sender sends a packet and **starts a timer**.
2. The receiver **checks the packet for errors**.
3. If it is error free, the receiver sends a **positive acknowledgement** back; the sender then **sends the next packet**.
4. If the sender does **not receive an acknowledgement before the timer ends**, a **timeout** occurs ...
5. ... and the packet is **resent**, until an acknowledgement arrives (or a set number of attempts is reached).

With a **negative acknowledgement** the receiver instead sends a message back when a packet **has an error**, asking for it to be resent.

8 Check digit

A **check digit** finds errors in **data entry** (typing or scanning a number), not in transmission. It is an extra digit added to the end of a code such as a barcode or an ISBN (book number).

GENERAL METHOD **Check digit**

1. The check digit is **calculated from the other digits** using an **algorithm** and **added to the end** of the code.
2. When the code is **entered or scanned**, the check digit is **recalculated** using the **same algorithm**.
3. If the calculated digit **does not match** the check digit in the code, an **error** has occurred (e.g. a digit typed wrongly, or two digits swapped).

EXAMPLE **Find the check digit for the ISBN 978030640615. Multiply the digits by 1, 3, 1, 3 …, add them, then the check digit is the number that makes the total up to the next multiple of 10.**

Weights 1 and 3 alternate.

$9\times1 + 7\times3 + 8\times1 + 0\times3 + 3\times1 + 0\times3 + 6\times1 + 4\times3 + 0\times1 + 6\times3 + 1\times1 + 5\times3$

$= 9 + 21 + 8 + 0 + 3 + 0 + 6 + 12 + 0 + 18 + 1 + 15 = 93$

next multiple of 10 is 100: $100 - 93 = 7$

ANSWER **check digit 7: ISBN 9780306406157**

TRY IT YOURSELF

1. Which error detection method is used for data entry rather than transmission?
2. Which method sends a copy of the data back to the sender?
3. In ARQ, what happens if no acknowledgement arrives before the timer ends?

9 Summary

- Errors: data lost, gained or changed, by interference, crosstalk, skewing, collisions.
- Parity: parity bit makes the number of 1s odd / even; receiver recounts. Misses even numbers of flips and transpositions.
- Parity block: parity bit per byte + parity byte per column; the bad row and column locate (and correct) the bit.
- Checksum: value calculated by an algorithm, sent with the data, recalculated and compared.
- Echo check: receiver sends a copy back; sender compares.
- ARQ: acknowledgement + timer; no acknowledgement → timeout → resend.
- Check digit: data ENTRY; calculated from the digits, recalculated on entry, compared.

IF YOU SEE …

"an odd or even process"	→ parity check
"a value calculated … before and after transmission"	→ checksum
"a copy is sent back"	→ echo check
"acknowledgement and timeout"	→ ARQ
"a value appended … checked on data entry"	→ check digit

PART 2

How it is examined

Question types, what the examiner gives marks for, and real past-paper questions solved.

10 Ways they test it

TYPE 1 How errors occur

> *"Describe how an error can occur in the data during transmission" [2-3]*

Spot it "how errors occur".

1. A cause (interference / crosstalk / skewing) AND its effect (data lost, gained or changed).

TYPE 2 Name the method

> *a table of statements to name [5]; "tick the method that does not use a calculated value" [1]*

Spot it "identify".

1. Use the trigger phrases in the summary. The echo check is the one with no calculated value.

TYPE 3 Describe a method

> *"Explain how the odd parity check detects errors" [4]; "describe the checksum process" [5]; "explain how ARQ operates using positive acknowledgement" [5]*

Spot it "explain how ... detects".

1. Write the method steps in order: before sending, during, after, compare, what happens if wrong.

TYPE 4 Parity bits

> *"Give the parity bit for each byte" [3]; "identify the byte with an error"*

Spot it a byte table.

1. Count the 1s in the data bits; for odd parity add a bit so the total is odd.

TYPE 5 **Limits of parity**

> *"Explain why the error may not be detected" [2]*

Spot it "not detected".

1. Two bits flipped / swapped (transposition) → the number of 1s is still odd / even → it still meets the parity.

11 What the examiner looks for

"Explain how the odd parity check detects errors" [4]

Marking points (one mark each, up to the marks shown)

- The number of 1s / 0s is counted
- A parity bit is added to each byte / 7 bits before transmission …
- … to make the number of 1s in each byte odd
- After transmission, if the number is odd no error is detected
- After transmission, if the number is even an error is detected

KEYWORDS **parity bit** **count the 1s** **odd** **after transmission**

"Describe the process of the checksum error detection method" [5]

Marking points (one mark each, up to the marks shown)

- The checksum is calculated from the data …
- … using an algorithm
- The checksum value is transmitted with the data
- The checksum is recalculated after transmission / by the receiver
- If the values do not match an error is detected // if they match no error
- … the data is requested to be resent if there is an error

KEYWORDS **algorithm** **transmitted with the data** **recalculated** **compared**

Wording trap · Check digit vs transmission

THE QUESTION **0478/12/M/J/26 Q4** ↗ Paper 1 · Computer systems **2 marks**

An odd parity byte check is used. There is an error that is not detected. Identify two other error detection methods that could be used.

✓ CREDITED

- Parity block check
- Checksum
- Echo check
- ARQ

✗ NOT CREDITED

- check digit

WHY

A check digit is for data ENTRY. This question is about transmission, so it is not accepted.

From: 0478/12/M/J/26 Q4(b)(ii) mark scheme

12 Past-paper questions, solved

0478/12/M/J/24 Q6 ↗ Paper 1 · Computer systems **5 marks** ⤢ Full size

6 The table contains statements about error detection methods.

Complete the table by giving the correct error detection method for each statement.

error detection method	statement
.....	An odd or even process can be used.
.....	A value is calculated from the data, using an algorithm. This happens before and after the data is transmitted.
.....	A copy of the data is sent back to the sender by the receiver.
.....	Acknowledgement and timeout are used.
.....	A value is appended to data that has been calculated using the data. This value is checked on data entry.

Swipe sideways to read the whole question

How to start Match each statement to its trigger phrase: odd or even, value calculated before and after, copy sent back, acknowledgement and timeout, value appended and checked on data entry.

▾ Show a full-mark answer and the mark scheme · official marking

WHAT TO WRITE

parity check · checksum · echo check · automatic repeat query (ARQ) · check digit

PART	ANSWER / WORKING	MARKS	GUIDANCE
6	parity (check / bit / byte / block) · checksum · echo check · ARQ · check digit, one mark each	B5	

Total: 5 marks

0478/11/O/N/23 Q4 ↗ Paper 1 · Computer systems **5 marks** ⤢ Full size

4 Data is transmitted between a computer and a printer.

(b) An odd parity check is used to detect errors in the data transmission.

Explain how the odd parity check detects errors.

..... [4]

(c) Another error detection method sends the data from the computer to the printer, then a copy of the data received is sent back from the printer to the computer. The two sets of data are compared to see if they match.

State the name of this type of error detection method.

..... [1]

Swipe sideways to read the whole question

How to start (b) is the five steps of the parity method; four of them earn the marks. (c) "a copy … sent back" = echo check.

▼ Show a full-mark answer and the mark scheme · official marking

WHAT TO WRITE

(b) Before transmission the number of 1s in each 7 bits is counted, and a parity bit is added to each byte to make the number of 1s odd. After transmission the receiver counts the 1s in each byte. If the number is odd, no error is detected; if it is even, an error is detected.

(c) Echo check.

PART	ANSWER / WORKING	MARKS	GUIDANCE
4(b)	Any four: number of 1s counted · parity bit added to each byte before transmission · … to make the number of 1s odd · after transmission odd = no error · even = error detected	B4	
4(c)	Echo (check)	B1	

Total: 5 marks

5 Errors can occur when data is transmitted.

(a) Give **one** reason an error may occur when data is transmitted.

..... [1]

(b) Some error detection methods use a calculated value to check for errors.

Tick (✓) **one** box to show which error detection method does **not** use a calculated value to check for errors.

A Check digit ☐

B Checksum ☐

C Echo check ☐

D Parity check ☐

[1]

(c) An automatic repeat request (ARQ) can be used to make sure that data is received free of errors. It can use a positive or negative acknowledgement method to do this.

Explain how an ARQ operates using a positive acknowledgement method.

..... [5]

Swipe sideways to read the whole question

How to start (c) is the ARQ method: timer, check, acknowledgement, next packet, timeout, resend.

▼ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

(a) Interference.

(b) C (echo check).

(c) When the sender transmits a packet it starts a timer. The receiver checks the packet for errors. If it is error free, the receiver sends an acknowledgement back to the sender, and the next packet is sent. If the sender does not receive an acknowledgement before the timer ends, a timeout occurs and the packet is resent, until an acknowledgement is received.

PART	ANSWER / WORKING	MARKS	GUIDANCE
5(a)	interference // crosstalk	B1	
5(b)	C	B1	
5(c)	Any five: timer started on sending · receiver checks for errors · acknowledgement sent if error free · next packet sent · no acknowledgement before timer ends … · timeout · packet resent · until acknowledged / max attempts	B5	

Total: 7 marks

0478/12/O/N/24 Q5 ↗ Paper 1 · Computer systems — **4 marks** — ⤢ Full size

5 A barcode scanning system uses a check digit to check for errors in data on input.

(a) Explain how the barcode scanning system operates to check for errors.

..... [4]

Swipe sideways to read the whole question

How to start Follow the method: calculated, added, recalculated on scanning with the same algorithm, compared.

▼ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

A check digit is calculated from the barcode digits using an algorithm (e.g. modulo 11) and added to the end of the barcode. When the barcode is scanned, the check digit is recalculated using the same algorithm. If the recalculated digit does not match the check digit, an error has occurred in scanning; if they match, there is no error.

PART	ANSWER / WORKING	MARKS	GUIDANCE
5(a)	Any four: calculated from the barcode data · using an algorithm (e.g. modulo 11) · added to the barcode · recalculated when scanned · same algorithm · do not match = error / match = no error	B4	

Total: 4 marks

13 Common mistakes

✗ "The parity bit makes the byte odd"

✓ "... makes the NUMBER OF 1s in the byte odd"

✗ "A checksum is the number of 1s"

✓ "A value calculated from the data using an algorithm"

Counting 1s is parity.

✗ Check digit for a transmission question

✓ Parity, checksum, echo check or ARQ

Check digit = data entry only.

✗ "ARQ checks the data" and nothing else	✓ Timer · acknowledgement · timeout · resend

The marks are for the process.

14 Practice

Practice: easy, medium, hard

1. Give the even parity bit for 101 1000.
2. Name the error detection method that uses acknowledgement and timeout.
3. Give two ways data can be affected by an error in transmission.
1. Describe how an echo check works. [3]
2. Find the checksum for byte values 120, 64 and 100 (add, remainder after 256).
3. Give one limitation of a parity byte check.
1. Explain how a parity block check finds AND corrects a single-bit error. [4]
2. A barcode 978030640615 is typed as 978030460615 (two digits swapped). Explain how the check digit 7 shows the error.

15 Can I do this?

0 / 5 ticked

- [ ] I can say how errors occur in transmission.
- [ ] I can add parity bits and explain parity byte and parity block checks.
- [ ] I can describe checksum and echo check.
- [ ] I can describe ARQ with positive acknowledgement and timeout.
- [ ] I can describe how a check digit works and calculate one.

Anything unticked: revise that section first (each line links to it). All ticked: take the quiz.

Answers

Answers to the "Try it yourself" and practice questions on this page. Try every question first.

Try it yourself 1

1.

ANSWER 1 (three 1s, so add a 1 to make four)

2.

ANSWER 0 (three 1s is already odd)

3.

ANSWER No: the number of 1s is still odd / even, so it still matches the parity

Try it yourself 2

1.

ANSWER Check digit

2.

ANSWER Echo check

3.

ANSWER A timeout occurs and the packet is resent

Practice: easy, medium, hard

Easy 1.

ANSWER 1 (three 1s, add one to make four)

Easy 2.

ANSWER ARQ (automatic repeat query)

Easy 3.

ANSWER Two of: lost, gained, changed

Medium 1.

ANSWER

Receiver sends a copy of the data back; sender compares it with the original; if they don't match an error is detected

Medium 2.

1. 120 + 64 + 100 = 284
2. 284 − 256 = 28

ANSWER **28**

Medium 3.

ANSWER

It cannot detect two bits changing / a transposition; it cannot locate which bit is wrong

Hard 1.

ANSWER

Each byte has a parity bit; a parity byte is added for each column; the receiver checks every row and column; the bad row and bad column cross at the wrong bit, which is flipped

PART	ANSWER / WORKING	MARKS	GUIDANCE
	parity bit per byte	B1	
	parity byte / column parity	B1	
	row and column checked	B1	
	bit where they cross is the error → corrected	B1	
			Total: 4 marks

Hard 2.

ANSWER

The check digit is recalculated from the typed digits with the same algorithm; it no longer equals 7, so an error is detected

NOTE 4

Encryption: symmetric and asymmetric

1 In this note

SYLLABUS 2.3 ENCRYPTION

- 2.3.1 Understand the **need for and purpose of encryption** when transmitting data.
- 2.3.2 Understand how data is encrypted using **symmetric** and **asymmetric** encryption.

Before this: Error detection. Next chapter: Hardware.

PART 1

Learn the topic

The notes: every idea from the start, with our own examples.

2 What you should already know

Packets travel through many devices

A packet passes through many routers on the internet. Any of them, or a hacker listening on the network, could read it.

Quick check: can a packet be intercepted on its way?

Yes.

3 Why data is encrypted

Data sent across a network can be **intercepted**: a third party captures it on the way (e.g. with packet sniffing software). Encryption does not stop the interception, but it makes the data **meaningless** to anyone who does not have the key.

Encryption uses an **algorithm** and a **key** to scramble the **plain text** (the readable data) into **cipher text** (scrambled, meaningless data). **Decryption** uses a key to turn the cipher text back into plain text.

Plain text: the original, readable data. **Cipher text**: the encrypted, scrambled data. **Key**: a value used by the encryption algorithm to encrypt or decrypt the data.

EXAMPLE **A very simple encryption algorithm shifts each letter along the alphabet. The key is 3. Encrypt SEND HELP.**

Move each letter 3 places on: S → V, E → H ...

S E N D → V H Q G

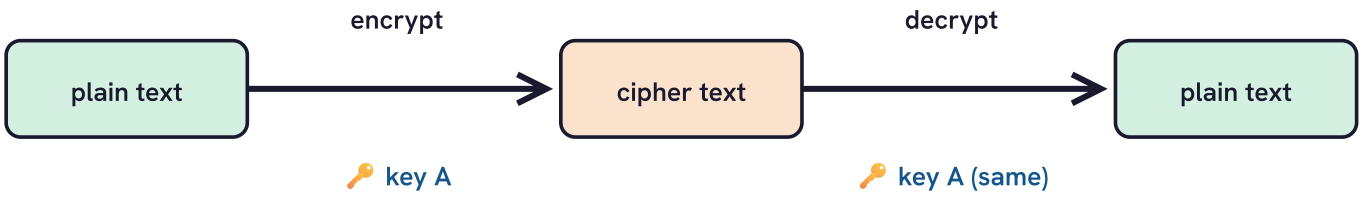
H E L P → K H O S

ANSWER **VHQG KHOS**

Anyone who intercepts VHQG KHOS sees nonsense. The receiver, who knows the key is 3, shifts each letter back 3 places to read it. Real encryption algorithms use keys that are hundreds of bits long, so they cannot be guessed.

4 Symmetric encryption

In **symmetric encryption** the **same key** is used to **encrypt and decrypt** the data.



the key must be shared with the receiver first

Symmetric: one shared key.

GENERAL METHOD **How symmetric encryption works**

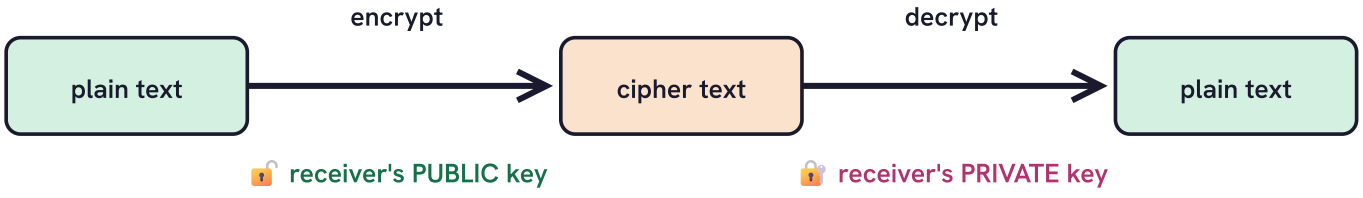
1. A **key** is generated (using an algorithm).
2. The sender uses the key and an **encryption algorithm** to turn the **plain text into cipher text**.
3. The cipher text is transmitted.
4. The **key is also sent** to the receiver (separately).
5. The receiver uses the **same key** to decrypt the cipher text back into plain text.

✗ COMMON MISTAKE

The weakness: the key itself has to be sent to the receiver. If the key is intercepted, anyone can decrypt the data.

5 Asymmetric encryption

Asymmetric encryption uses **two different keys** that are a matched pair: a **public key** and a **private key**. Data encrypted with the public key can **only be decrypted with the matching private key**.



anyone can have the public key; only the receiver has the private key

Asymmetric: the receiver's public key encrypts, only the receiver's private key decrypts.

GENERAL METHOD

How asymmetric encryption works

1. The receiver has a key pair. The **public key** is given to **anyone** who asks; the **private key** is kept **secret** and never sent.
2. The sender gets the receiver's public key and uses it to **encrypt** the plain text into cipher text.
3. The cipher text is transmitted. The public key **cannot decrypt** it.
4. The receiver uses their **private key** to **decrypt** the cipher text.

	Symmetric	Asymmetric
Keys	**one key**, shared	**two keys**: public and private
Encrypt with	the shared key	the **public key**
Decrypt with	the same shared key	the **private key**
Who knows the keys	sender and receiver both know the key	anyone can know the public key; **only the receiver knows the private key**
Security	the key must be sent, so it could be intercepted	**more secure**: the private key is never sent (**no key exchange**)
Speed	faster	slower (more complex)

TRY IT YOURSELF

1. What is the encrypted, scrambled data called?
2. In asymmetric encryption, which key decrypts the data?
3. Give the purpose of encryption.

6 Summary

- Purpose: if data is intercepted, it is meaningless / cannot be understood. Encryption does not stop interception.
- Encryption: algorithm + key turn plain text into cipher text; decryption turns it back.
- Symmetric: one shared key encrypts and decrypts; the key must be sent, so it could be intercepted.
- Asymmetric: public key encrypts, private key decrypts; the private key is never sent, so it is more secure.

IF YOU SEE …

"purpose of encryption"	→ if intercepted · cannot be understood / meaningless
"how symmetric works"	→ same key encrypts and decrypts · plain → cipher · algorithm · key sent to receiver
"differences symmetric / asymmetric"	→ one shared key vs public + private · public encrypts, private decrypts · who knows them

PART 2

How it is examined

Question types, what the examiner gives marks for, and real past-paper questions solved.

7 Ways they test it

TYPE 1 **Purpose**

> *"State the purpose of encrypting data" [1]*

Spot it "purpose".

1. "If it is intercepted, it cannot be understood." Not "to stop hackers" (it does not stop interception).

TYPE 2 **Describe a type**

> *"Explain how data is encrypted using symmetric encryption" [4]*

Spot it "symmetric" or "asymmetric".

1. Start with the key fact (same key / public + private), then the method steps.

TYPE 3 **Differences**

> *"Describe the differences between symmetric and asymmetric encryption" [4]*

Spot it "differences".

1. Points from both columns of the comparison table.

TYPE 4 **Cloze**

> *"Complete the paragraph about asymmetric encryption" [4-8]*

Spot it a word list.

1. Words to expect: algorithm, plain text, cipher text, meaningless, public, private.

TYPE 5 **Why asymmetric**

> *"Give one reason a person would use asymmetric instead of symmetric" [1]*

Spot it "instead of".

1. More secure // no need to exchange (send) the key.

8 What the examiner looks for

"Describe the differences between symmetric and asymmetric encryption" [4]

Marking points (one mark each, up to the marks shown)

- Symmetric has a shared key ...
- ... to encrypt and decrypt
- Both the sender and receiver know the key
- Asymmetric has different keys // a public key and a private key
- ... the public key encrypts the data and the private key decrypts it
- ... anyone can know the public key but only the intended receiver knows the private key

KEYWORDS **same key** **public key** **private key** **encrypt** **decrypt**

"Explain how data is encrypted using symmetric encryption" [4]

Marking points (one mark each, up to the marks shown)

- The data is encrypted and decrypted using the same key (1 mark), then any three:
- Plain text is encrypted into cipher text // cipher text is decrypted into plain text
- Data is encrypted using an algorithm ...
- ... that uses a key
- The key can be generated using an algorithm
- The key is transmitted to the receiver

KEYWORDS **same key** **plain text** **cipher text** **algorithm**

Wording trap · Purpose of encryption

THE QUESTION **0478/12/F/M/24 Q7** ↗ Paper 1 · Computer systems **1 mark**

State the purpose of encrypting data.

✓ CREDITED

- If the data is intercepted, it cannot be understood
- to make the data meaningless (to a third party)

✗ NOT CREDITED

- to stop the data being intercepted
- to stop hackers
- to keep it safe (alone)

WHY

Encryption does not prevent interception; it makes intercepted data useless.

From: 0478/12/F/M/24 Q7(a)(i) mark scheme

9 Past-paper questions, solved

0478/12/M/J/24 Q2 ↗ Paper 1 · Computer systems **5 marks** ⤢ Full size

2 Data can be transmitted from one device to another.

(c) Data is often encrypted when it is transmitted from one device to another.

(i) Explain how data is encrypted using symmetric encryption.

..... [4]

(ii) Give the purpose of encryption.

..... [1]

Swipe sideways to read the whole question

How to start (i) One mark is reserved for "same key": say it first. Then three steps of the method.

▾ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

(c)(i) The data is encrypted and decrypted using the same key. The plain text is encrypted into cipher text using an encryption algorithm that uses the key. The key is generated using an algorithm and is transmitted to the receiver, who uses it to decrypt the cipher text back into plain text.

(c)(ii) To make the data meaningless if it is intercepted.

PART	ANSWER / WORKING	MARKS	GUIDANCE
2(c)(i)	same key to encrypt and decrypt (1) + any three: plain text → cipher text · algorithm … · … that uses a key · key generated by an algorithm · key transmitted to the receiver	B4	
2(c)(ii)	to help keep the data secure // to make the data meaningless	B1	

Total: 5 marks

0478/12/F/M/24 Q7 ↗ Paper 1 · Computer systems — **5 marks** — ⤢ Full size

7 Data is transmitted using the internet.

(a) The data is encrypted before transmission.

(i) State the purpose of encrypting data.

..... [1]

(ii) Describe the differences between symmetric and asymmetric encryption.

..... [4]

Swipe sideways to read the whole question

How to start (ii) needs points about BOTH types. Two about symmetric, two about asymmetric is a safe plan.

▼ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

(a)(i) If the data is intercepted, it cannot be understood.

(a)(ii) Symmetric encryption uses one shared key to both encrypt and decrypt, and both the sender and receiver know it. Asymmetric encryption uses two different keys, a public key and a private key: the public key encrypts the data and the private key decrypts it. Anyone can know the public key, but only the receiver knows the private key.

PART	ANSWER / WORKING	MARKS	GUIDANCE
7(a)(i)	if intercepted, it cannot be understood	B1	
7(a)(ii)	Four from: shared key … · … to encrypt and decrypt · both know the key · public and private key · public encrypts, private decrypts · anyone can know the public key, only the intended receiver the private key	B4	

Total: 5 marks

6 Data can be encrypted using asymmetric encryption.

(a) Complete the paragraph about asymmetric encryption.

Use the terms from the list.

Some of the terms in the list will **not** be used. You may use a term more than once.

algorithm binary cipher text compression error
hardware hexadecimal meaningless plain text private
public readable transmission unreadable

Data is encrypted using an encryption key. This is a type of ..... that scrambles the ..... and turns it into ..... . This makes the data ..... . A ..... key is used to encrypt the data. This key cannot be used to decrypt the data. A ..... key is used to decrypt the data. Any device is able to request the ..... key, but only your device knows the ..... key.

[8]

(b) Data can also be encrypted using symmetric encryption.

Give **one** reason why a person would use asymmetric encryption instead of symmetric encryption.

.....

..... [1]

Swipe sideways to read the whole question

How to start Read the whole paragraph first. Two gaps must be opposite keys (public / private). The last sentence tells you which key anyone can request.

▼ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

(a) algorithm · plain text · cipher text · meaningless · public · private · public · private

(Data is encrypted using an encryption key. This is a type of **algorithm** that scrambles the **plain text** and turns it into **cipher text**. This makes the data **meaningless**. A **public** key is used to encrypt the data ... A **private** key is used to decrypt the data. Any device is able to request the **public** key, but only your device knows the **private** key.)

(b) It is more secure, because the private key is never sent.

PART	ANSWER / WORKING	MARKS	GUIDANCE
6(a)	algorithm · plain text · cipher text · meaningless · public/private · private/public (opposite) · public · private	B8	
6(b)	more secure // no need to worry about key exchange	B1	

Total: 9 marks

10 Common mistakes

✗ "Encryption stops data being intercepted" ✓ "Intercepted data cannot be understood"

✗ "Asymmetric: the private key encrypts" ✓ "The public key encrypts, the private key decrypts"

For sending data to someone.

✗ "Encryption is a key" ✓ "An algorithm that uses a key"

✗ "Coded" instead of "cipher text" ✓ "Cipher text"

Use the exact term.

11 Practice

Practice: easy, medium, hard

1 What is unencrypted, readable data called?

2 How many keys does symmetric encryption use?

3 Encrypt CAT with the shift-3 algorithm.

1 Explain why symmetric encryption is less secure than asymmetric. [2]

2 Describe how asymmetric encryption keeps an email secret. [3]

3 Decrypt KHOOR (shift-3 algorithm).

1 A bank sends account details to a customer. Explain why encryption is needed and which type is most suitable. [4]

12 Can I do this?

0 / 3 ticked

- [ ] I can state the purpose of encryption correctly.
- [ ] I can explain symmetric encryption.
- [ ] I can explain asymmetric encryption and compare it with symmetric.

Anything unticked: revise that section first (each line links to it). All ticked: take the quiz.

Answers

Answers to the "Try it yourself" and practice questions on this page. Try every question first.

Try it yourself 1

1.

ANSWER Cipher text

2.

ANSWER The private key

3.

ANSWER If the data is intercepted it cannot be understood / is meaningless

Practice: easy, medium, hard

Easy 1.

ANSWER Plain text

Easy 2.

ANSWER One (the same key encrypts and decrypts)

Easy 3.

ANSWER FDW

Medium 1.

ANSWER

The key has to be sent to the receiver, so it could be intercepted; the private key in asymmetric is never sent

Medium 2.

ANSWER

Sender encrypts with the receiver's public key; cipher text sent; only the receiver's private key can decrypt it

Medium 3.

ANSWER HELLO

Hard 1.

ANSWER

The data could be intercepted; encryption makes it meaningless to a third party; asymmetric is more suitable: the public key encrypts, only the private key decrypts and it is never sent, so no key exchange can be intercepted

PART	ANSWER / WORKING	MARKS	GUIDANCE
	data could be intercepted	B1	
	meaningless / cannot be understood	B1	
	asymmetric	B1	
	private key never sent // no key exchange	B1	

Total: 4 marks