

Cambridge

Lower Secondary

 Cambridge Assessment
International Education

Endorsed for full syllabus coverage

Computing

8

Ben Barnes
Margaret Debbadi
Pam Jones
Tristan Kirkpatrick

SERIES EDITOR:

Lorne Pearcey

 Boost

 **HODDER**
EDUCATION



Contents

Introduction	4
8.1 Building networks: Network structure and security	8
8.2 It's all in the planning: Pseudocode and algorithms	32
8.3 Let's talk technology: What's going on inside	61
8.4 Testing conditions: Developing games	93
8.5 Data input: Data collection and validation	127
8.6 Iterating through a solution: Software design and development	163
Glossary	195
Index	199
Acknowledgements	203



Introduction

About this book

Computer science is the study of computers, computing hardware and software, computer networks and the design of computer programs. It also includes the study of the way humans interact with computers and computing technology.

Computer science is linked to all areas of the world you live in today. It helps you to make positive changes to the world you live in, and provides important tools and **applications** to help you solve a wide range of problems. Computer science is continually evolving to provide new and valuable ways of improving your life and your interactions with the world around you.

This Student's Book will help you to understand some of the key areas of computer science, such as:

- cyber security
- **algorithms** and programs
- robotics, **artificial intelligence** and **augmented reality**
- gaming
- **databases** and **spreadsheets**
- software development.

This book also supports the learning objectives within the five strands of the Cambridge Lower Secondary Computing framework:

- **Computational thinking** is built into the tasks in this book. It looks at how computing can be used to explore and analyse data collected from the world around you. It is also about the development of skills to support problem-solving, for example how to describe a problem, and the data needed to solve that problem, in a way that a computer can understand.
- **Programming** explores the steps involved in designing and creating a computer program that can be used to carry out a particular task. In this book, you will study **text-based programming** languages such as Python and explore how to program a physical computing device to solve a problem.
- **Managing data** looks at how computers and computer programs can be used to store, organise and manage different types of data. It also explores how that data can be used to support problem-solving. In this book, you will learn how to use, edit and create databases and spreadsheets to help with managing different types of data.
- **Networks and digital communication** focuses on the methods used to transfer digital data between different computing devices, and how these devices are used to support communication. In this book, you will explore how different computing devices can be linked together to support data transfer.
- **Computer systems** is about how computer hardware devices and computer programs work together to support users in solving problems. It involves considering how the hardware and software and the data input is **processed**, stored and then output, to help a user solve a problem. In this book, you will explore the network and communications devices used to transmit data and information around a computer, and the world, in the process of solving a problem.

KEYWORDS

applications software: the software that users access to carry out tasks

algorithm: step-by-step instructions to solve a particular problem

artificial intelligence (AI): the study of machines and algorithms designed to carry out tasks in a way that is similar to humans

augmented reality (AR): a simulation that superimposes digital images on the user's real-world environment and allows the user to interact with those images

database: an application that is used to organise data that can then be stored, processed and accessed electronically

spreadsheet: an application that uses rows and columns to organise data and carry out calculations using that data

text-based programming: programming that requires the programmer to type text, e.g. Python

process: carrying out an operation on data, e.g. querying a database or doing a calculation using data in a spreadsheet

This Student Book has six units:

8.1 Building networks: Network structure and security builds on skills developed in Stage 7, investigating ways in which devices can communicate over networks. The unit provides an insight into the threats to networks that exist and the ways in which skilled engineers can protect against them. You will explore ways that networks can be structured and built, including the essential hardware and software required for scalability.

8.2 It's all in the planning: Pseudocode and algorithms develops knowledge and skills using MicroPython with the BBC micro:bit, including sending a message from one micro:bit to another. You will plan an algorithm and program with MicroPython to send an image, text and numbers and use ASCII to send a message.

8.3 Let's talk technology: What's going on inside provides an insight into the different types of software that support interaction with digital devices. It also covers the various types of computer memory; how files can be reduced in size; converting between binary and denary numbers; and using truth tables to model logic gates. You will investigate newer areas of computing such as robotics, artificial intelligence and augmented reality.

8.4 Testing conditions: Developing games allows you to develop your Python programming skills, focusing on the use of sequencing and selection. You will decompose a complex problem and develop a game that meets a brief.

8.5 Data input: Data collection and validation builds on knowledge and skills developed in Stage 7 where real-life situations were modelled using MS Access and MS Excel. You will study how to incorporate automatic checks into database and spreadsheet models, how to design data-capture forms and how to link data elements in a spreadsheet using formulae. Finally, you will investigate how to use a spreadsheet data model to ask what-if questions and make predictions.

8.6 Iterating through a solution: Software design and development focuses on the flow of a project and iterative development from start to finish. You will learn about using selection in Python to create a question-based quiz to determine whether or not an item can be recycled. You will develop the solution iteratively, from planning with algorithms through to programming with Python.

How to use this book

In each unit, you will learn new skills by completing a series of tasks.

These features appear in each unit:

Get started!

This box introduces the unit and asks you some questions to discuss in pairs or a small group.

Learning outcomes

This box lists the learning outcomes that you will cover in the unit.

Warm up

This box provides a task to do in pairs or a small group to get the learning started.

SCENARIO

This box contains a scenario that puts the tasks in the unit into a real-world context.

Do you remember?

This box lists the skills you should already have before starting the unit.

DID YOU KNOW?

This box provides an interesting or important fact about the task or theme.

Learn

This box introduces new concepts and skills.

Practise

This box contains tasks to apply and practise the new skills and knowledge from the 'Learn' box.

Go further

This box contains tasks to enhance and develop the skills you have previously learned in the unit.

Challenge yourself

This box provides challenging tasks with additional instructions to support new skills.

Final project

This box contains a final project that encompasses all the skills you have developed over the unit, in the context of the Scenario. The tasks in this box can be used to support teacher assessment of the learning objectives from the Learning outcomes box.

Evaluation

This box provides guidance on how to evaluate and, if necessary, test the final project tasks.

What can you do?

This box provides a summary of the skills you have learned in the unit and can be used to support self/peer assessment of the learning objectives.

Computational thinking

Most computational thinking skills are embedded into the 'Practise' tasks. However, where you see this box, an individual computational thinking skill is highlighted for your attention.

KEYWORDS

Important words are shown in **emboldened orange font** and are defined in this box. They also appear in the glossary at the back of the book.

Speech bubbles provide hints and tips as you complete the tasks.

Student resource files, used in some of the Practise boxes, are available at www.hoddereducation.com/cambridgeextras

Unit 8.1

Building networks: Network structure and security

Get started!

In this unit, you will take a close look at the ways in which devices can communicate over networks, including the hardware and software components required to make this happen. Safety and security of data transmission are crucial for modern networks and you will investigate methods of keeping them secure.

Discuss the following with your partner:

- What are the different methods of data transmission on a network?
- Which is the fastest wireless data-transmission method?
- How can you ensure that data cannot be intercepted?

In this unit, you will develop your understanding of ways in which network technology can improve transmission and keep you safe while using networks.



Learning outcomes

In this unit, you will learn to:

- identify different types of network, such as PAN, LAN and WAN
- identify the type of network that should be used in different scenarios
- describe the uses and characteristics of copper and fibre-optic cables to transmit data
- describe the advantages and disadvantages of wired and wireless networks
- describe the advantages of security features in different types of networks
- describe how echo checks are used to detect errors in transmission
- explain how firewalls protect a network and why they are important
- explain how antivirus and anti-spyware software provides protection to keep data secure on a network
- explain the security features used by different types of networks
- explain the purpose of operating systems and describe some of the main tasks an operating system carries out
- explain what a network operating system is
- explain why a network operating system is labelled 'utilities software'
- identify and describe how augmented reality is used in education, gaming and robotics
- follow a flowchart that uses conditional statements to illustrate how error checks work.

Warm up

All devices connected to a network have a unique IP address. The devices below, which are yet to be assigned IP addresses, are all part of the same network.

Complete the table to assign valid IP addresses to the devices. The devices that you need to assign addresses to are listed on the left-hand side of the table. Make up the IP addresses, remembering to ensure that they follow the rules of an IP address.

Device	IP address
Router	192.168.1.1
Smart TV	
Laptop	
Tablet computer	
PC	

Remember: IP addresses are made up of four sets of three numbers between 0 and 255.

SCENARIO

A youth group working in the community is setting up technology centres for young people to meet, play games (including augmented-reality games) and socialise in a safe, supervised environment. The technology centres will be based in local community centres.

The youth group's aim is to help educate young people with steps that they can take to keep their digital devices and online activity secure.

It has employed you as its new network security and communications specialist. Your job is to advise the youth group on the types of network, telecommunications links, technology and software that it will require in the community centres to help keep the young people safe while they are using their own devices.

You are also responsible for helping the youth group organisers learn about networks, telecommunications and data security before it opens its first community group in your local area.

DID YOU KNOW?

A cyber-attack happens about once every 39 seconds worldwide.

Do you remember?

Before starting this unit, you should be able to:

- ✓ explain different ways in which devices can transmit data
- ✓ understand how a DNS enables users to access websites on their devices and explain the steps a DNS takes
- ✓ understand how IP addresses and web servers work
- ✓ explain what the structure of a URL looks like and identify the different parts

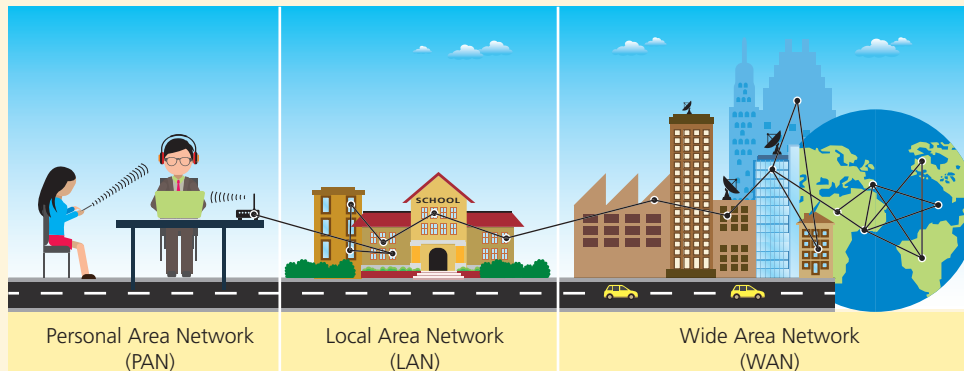
- ✓ explain what types of encryption can be used on websites
- ✓ find information on the security certificates of a website
- ✓ understand how errors can occur in data transmission and apply ways to check that a message is sent correctly
- ✓ modify a program based on a basic cipher
- ✓ encode and decode messages using a cipher
- ✓ understand how search engines categorise data
- ✓ explain how AI is used to improve search-engine results.

Networking: It's not just about meeting people

Learn

Networking: it's not just about meeting people! **Networks** come in all shapes and sizes, from small networks between just two computers to large networks spanning the globe with thousands of devices connected to them.

There are three types of network that you need to be familiar with: PAN, LAN and WAN. Each type of network has its own advantages and disadvantages and uses. All network types allow devices to communicate, with the main difference being the geographic area that they cover.



Personal Area Networks (PAN) are the smallest type of network, usually connecting devices that are in close proximity to an individual. These are useful for smart watches, headsets and wireless headphones. PAN networks are usually connected via **Bluetooth**.

Local Area Networks (LAN) allow devices to communicate over a small geographic area, usually a single site, such as a single building, school or college.

Wide Area Networks (WAN) allow devices to communicate in the same way, but over a larger geographical area, and are usually made up of several LANs connected together. Companies often use this method if they have a number of different offices spread across a geographical region. The largest example of a WAN is the internet.

Lots of smart tech has emerged that provides new technologies to users. Robot vacuum cleaners, smart lawnmowers, smart fridges, smart doorbells and many other 'smart' devices provide convenience and extra functionality to users. Most of these devices are usable on a LAN.

It's often quite difficult to tell whether a device uses a PAN or a LAN. Remember that for a device to be on a PAN, it will work only when in close proximity to the device it is connected to; smart watches, wireless headphones and smart medical devices all work on PANs. Technologies such as smart light bulbs and plug sockets would be on a LAN because they can be accessed and switched on and off from anywhere on a local network, not just from one user's phone, for example.

Why network devices?

There are several benefits and drawbacks of networking devices.

Benefits	Drawbacks
<ul style="list-style-type: none"> ● Users can share devices such as printers and scanners. ● Users can share software licences (which means that software is often cheaper). ● Users can communicate with each other over the network. ● Users can share an internet connection. 	<ul style="list-style-type: none"> ● Networking hardware can be very expensive. ● Managing a network can be complicated and may need skilled people to manage it. ● Viruses can spread to all devices on the network if a single user's device becomes infected.

Smart devices often make use of networks. For example, if a user has a robot vacuum cleaner, the software that comes with the device allows the user to set the time of day that it cleans, which rooms it cleans and how powerful the suction should be. This functionality allows the cleaner to clean **autonomously**, as it has been programmed to adjust to the user's preferences the more they use it. This makes a user's life easier and completes tasks that otherwise the user would have to do.



Servers

A **server** is a computer that is usually very powerful and is connected to a network. Different types of server provide different services for the devices connected to them via the network. In Stage 7, you investigated the way in which web servers function, but a server can provide a number of other useful services.

- **File servers** offer devices on a network a place to store and access files. On large networks, files are often stored on the server, not on the device that the user is working on. This can be beneficial in a business where a number of people need to access the same files.
- **Print servers** enable devices on a network to share printers. If you imagine a large office, it would not be feasible for every device to have its own printer. A print server manages which devices can print to a single printer so that users can share it.

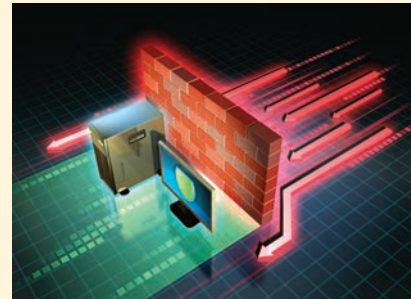


- **Mail servers** store email messages and allow users to **authenticate** themselves so that they can send and receive messages.
- **Web servers** provide internet-accessible files and transmit files to users over the world wide web.

Servers are also very important for maintaining the security of a network. **Antivirus, anti-spyware** and **firewall** applications on the server keep all the networked devices safe. You will investigate these security features in more detail in upcoming lessons. Servers co-ordinate the communication of devices on the network.

In the modern world, most devices form part of a network. In the home, even fridges, vacuum cleaners, lawnmowers and light bulbs can often be networked to increase their functionality.

Network operating systems: Just like regular systems, servers require an **operating system**. The type of operating system a network uses is usually more advanced, as it controls how network services are delivered to all the devices on the network.



KEYWORDS

network: a collection of computing devices connected to each other, either wired or wirelessly

Personal Area Network (PAN): a type of network that communicates over an area of no more than 10 metres, usually connecting smart devices within the immediate area of a user

Bluetooth: a wireless technology that allows data transmission using radio waves

Local Area Network (LAN): a type of network that communicates over a small geographical area, such as a single building

Wide Area Network (WAN): a type of network that communicates over a large geographical area, such as across a city or country

software: the programs or set of instructions that tell a computer what to do to complete a task; aspects of a device you cannot touch

hardware: the physical parts of a computer that you can touch and see, e.g. the processor, storage devices, input devices, output devices

autonomous programming: computer hardware and complex AI software working together to solve a problem without any human interaction

server: a computer that offers a service to other devices on a network, such as file-sharing services and printer-sharing services

authenticate: allowing a computer or a human to verify that the user is who they say they are

operating system: the systems software that manages hardware and software, giving the user an interface to operate the computer

antivirus: software that detects and removes viruses from a computer

anti-spyware: software that detects and removes spyware from a computer

firewall: software or hardware that prevents unauthorised access to a network

Practise

- 1 Using your knowledge of different networks, categorise the following scenarios into PAN, LAN or WAN:
 - a a home network containing three PCs, two laptops, one tablet, four mobile phones, three smart TVs, one smart vacuum cleaner and one games console
 - b a business with 5000 PCs in total across three different office blocks in three separate countries; all the devices are on the same network
 - c a smart fitness band that a runner wears, who also carries their mobile phone.
- 2 **a** Open the worksheet **PAN_LAN_WAN activity.docx** provided by your teacher. Investigate all the devices you can find that connect to a network. For each of the devices, identify which type of network it connects to. Add some devices to the list that you can find on either your home or school network. Complete the table on the worksheet.
 - b** Think about the answers to the questions below and be ready to feed back to your classmates.
 - i Why does networking devices increase the security risk?
 - ii Are there ways in which security risks can be prevented?
- 3 As a class, discuss the security implications of having so many networked devices in the home and at school.
- 4 How many of the networked devices people have in their homes automatically change how they operate based on how the people use them? Look at the list below and see whether you can expand it.

Device	How it changes based on how people use it
Smart speaker	Adjusts volume based on the surrounding noise or the time of day

Making connections

Learn

Hardware

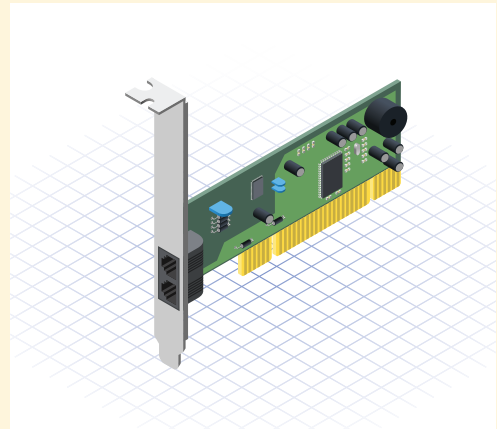
For networks to function properly, they need a number of different pieces of network hardware. Each piece of hardware has its own role to play in ensuring that the network functions correctly.

Servers

Servers provide services to a network. You investigated the functions that they can offer devices in the previous Learn box.

Network Interface Controller

A Network Interface Controller (NIC) must be present in a device to enable it to communicate with other devices over a network. Sometimes these are physical cards that can be plugged into a PC, but often they are built into a device using smaller electronic circuitry. Mobile phone NICs are much smaller than a PC NIC, for example. Every NIC has a MAC address that uniquely identifies the device on a network. The MAC address is assigned when the device is manufactured and cannot be changed.



Switch

A **switch** connects together multiple devices on a network. It stores the MAC address of every device that it is connected to. When one device wants to send **data** to another, it uses the MAC address to send the data only to the device that is meant to receive it. Often switches connect large numbers of devices together using **ethernet cables**.



Wireless Access Point

A **Wireless Access Point (WAP)** allows devices to connect to a network using Wi-Fi.

Router

A router connects different networks together and provides access to the internet. If you want to send data from one place to another, a router finds the fastest route to send the data.

All-in-one devices

Home networks often use an all-in-one device that combines a router with a WAP and switch. The WAP allows devices to connect to the network via Wi-Fi, and a four-port switch allows users to connect up to four devices directly to the network via an ethernet cable.

Wired vs wireless

The devices that make up a network can be connected in a variety of ways, all of which can be categorised into wired or wireless.

Wired connections

Wired connections use copper wire or fibre-optic cable. Fibre-optic cables are usually used to connect LANs together to form WANs across large geographic areas.

Copper wire: Copper wire, also known as **ethernet cable**, transmits data as electrical pulses and can transmit around 10 Gb per second. It is often used to connect devices on a LAN as it transmits data reliably over a distance of about 100 metres. Copper wire is fairly cheap but is prone to **interference**.

Fibre-optic cable: Fibre-optic cables transmit data as pulses of light, which is much faster than electrical signals. This means that they have a high **bandwidth** of up to 100 Tb per second, much faster than the copper alternative. Fibre-optic cables are not as prone to interference, so they are more reliable than copper cables.

Wired connections are often much more reliable and faster than wireless connections; however, they do have some drawbacks:

- Wired connections can be expensive to install. Imagine how much ethernet cable you would need to wire up every device to the network switches in your school!
- Devices connected via cabling are not portable, as they can move only as far as the wires will allow!

Wireless connections

The table shows the most common standards of wireless communication.

Method of wireless transmission	Bandwidth
Wi-Fi	The latest version of Wi-Fi is capable of transmitting data at 9.6 Gbps (9600 Mbps).
Bluetooth	Bluetooth is capable of transmitting data at 2 Mbps.
3G	The average speed of 3G is 3 Mbps.
4G	The average speed of 4G is between 8 and 10 Mbps.
5G	The average speed of 5G is 100 Mbps.

Wireless connections are great for convenience, but they have some drawbacks.

- Wireless networks are often subject to interference, which can prevent data from transmitting accurately.
- The data transmitted over a wireless network can be intercepted easily.
- Wireless networks are often slower than wired networks.



Different types of wireless networks fit into three categories: WPAN, WLAN and WWAN.

WPAN: A **Wireless Personal Area Network** is a type of PAN that can be connected using wireless technology only. This is most often Bluetooth, as a PAN generally does not need to connect to a device further than 10 metres away.

WLAN: **Wireless Local Area Networks** are often used in homes and in small businesses located in one building over a small geographical area. Here, devices connect to the WLAN using Wi-Fi, as the transmission distance of Wi-Fi is around 9 metres (or more without obstructions such as walls).

WWAN: **Wireless Wide Area Networks** are types of Wide Area Networks that are often used for telecommunications by mobile devices using 3G, 4G and 5G. Devices connect to a 'mast' or 'tower', which can be done over a distance of up to 15 kilometres.



Modern-day users require wide bandwidths, so that they can transfer large files quickly.

Augmented-reality gaming

Imagine that you are gaming **online**. Which of the technologies above would you use and why? Would a wired or wireless connection be best for gaming? Would you choose copper or fibre connection to the WAN?

Game designers are pushing the boundaries of what is possible in online gaming and they are introducing **augmented-reality** games to the market.

Augmented reality in gaming is an enhanced version of the real world, showing digital elements on top of what humans can already see. This type of game requires a lot of computing power, and involves large amounts of data being transmitted via networks. This means that the existing networks need to be improved and speeded up continually to be able to keep pace with the demands of the modern world.



Practise

Now you are going to build some networks.

- 1 For each of the scenarios below, draw the network hardware and devices on a large sheet of paper. Use coloured pens to represent the different types of connection methods according to the 'Connections key' below.

Connections key	
Ethernet cable	Red
Bluetooth connection	Blue
Wi-Fi connection	Purple
3G/4G/5G	Yellow
Fibre cable	Green

a Scenario 1

A small office (Office 1) has a LAN with five laptops connected via Wi-Fi, two printers connected via ethernet and five PCs connected via ethernet to the network. Two of the workers have smart watches that connect to their smartphones via Bluetooth. The two smartphones in the office do not connect to the Wi-Fi, but use 4G or 5G networks to communicate.

b Scenario 2

The main office in Scenario 1 is part of a larger office complex of two offices in total. Office 2 is much smaller than Office 1, and has two workers who both have a smartphone and a laptop. When the company built the offices, it wanted to make sure that they were future proof, so it installed a fibre-optic cable between the two offices.

- 2 Add the second office to your network diagram.
- 3 Now highlight which areas of the network are a PAN, LAN or WAN. Also show in the diagram any additional network hardware the offices may require (routers, switches, access points, and so on).
- 4 Would the network you have drawn be appropriate for the youth group in the Scenario at the start of this unit? Explain your answer to your partner.

KEYWORDS

switch: a network device that forwards data from one device to another

data: raw facts and figures

ethernet cable: a popular type of copper cable used to transmit data between devices

Wireless Access

Point (WAP): enables devices to connect to a network using Wi-Fi

interference: what happens when something interrupts the transmission of a signal; this could be a physical obstruction such as a wall, or other radio waves

bandwidth: a measure of the maximum number of bits that can be transmitted over a network or cable in a specified amount of time

online: connected to the internet

augmented reality (AR): a simulation that superimposes digital images on the user's real-world environment and allows the user to interact with those images

You said what?

Learn

Transmitting data

Networked devices transmit **binary** data, which consists of 1s and 0s. Eight bits of 1 or 0 make up a byte.

The devices transmit data using a wired or wireless method, and need to be able to do this extremely quickly, even for large amounts of data.

ASCII

ASCII is a set of codes that represent characters (for example, letters, numbers and punctuation marks) in a format a computer system can recognise. ASCII assigns each character a specific binary code. You will learn more about ASCII in Unit 8.3.

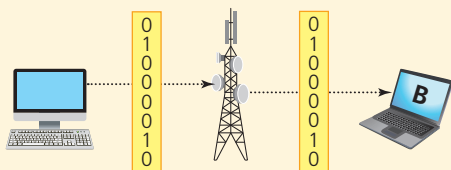
Character	Binary
A	01000001
B	01000010
C	01000011

Serial transmission

ASCII binary codes are 8 bits, or a byte. For example, '01000010' is the binary representation in ASCII of 'B'. In **serial transmission**, a device transfers one bit at a time to the receiving device.

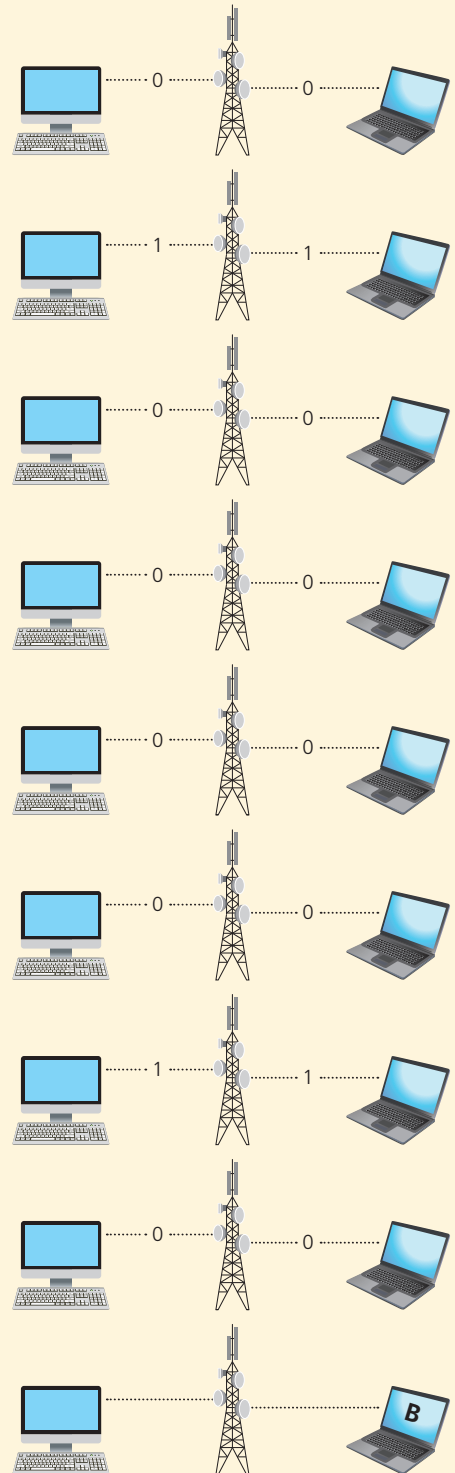
Parallel transmission

In **parallel transmission**, 8 bits, or 1 byte, of data can be sent simultaneously.



Transmission errors

When computers communicate, it is important that the information sent and received is correct. Take an air traffic control team in an airport, for example.



It is essential that the messages the controllers communicate to pilots are correct, otherwise an aeroplane could be landing on a runway before another plane has taken off, which would be a disaster.

Another example is in hospitals. Most hospitals have complex network structures that rely on data transmission to show how many beds they have available in various departments. If this is not accurate, people could be turned away from a hospital because the network showed that there were no beds available, when in fact there were.

Large skyscrapers often use network-connected carbon-monoxide and heat detectors. What if a computer mistakenly reported that a heat detector was cold, when there was a fire in the room it was monitoring?

People rely on computers to send data accurately across networks. Unfortunately, errors in systems do happen, but computers have some clever ways to find them quickly.

Why do errors occur?

When sending data over a network, there are a number of reasons why the data that is received could be incorrect. Imagine that a laptop wants to transmit the message '00000001' over a large WAN to a PC. Here are some examples of things that could cause an error:

- Interference to the Wi-Fi signal connecting the laptop to the network could cause one of the bits to **flip**.
- A **power surge** on one of the networked devices that the data is travelling through could cause a bit to flip.

How can errors be detected?

Echo checking ... Echo checking ... Echo checking.

When a computer receives data, it immediately returns it to the sending computer for comparison.

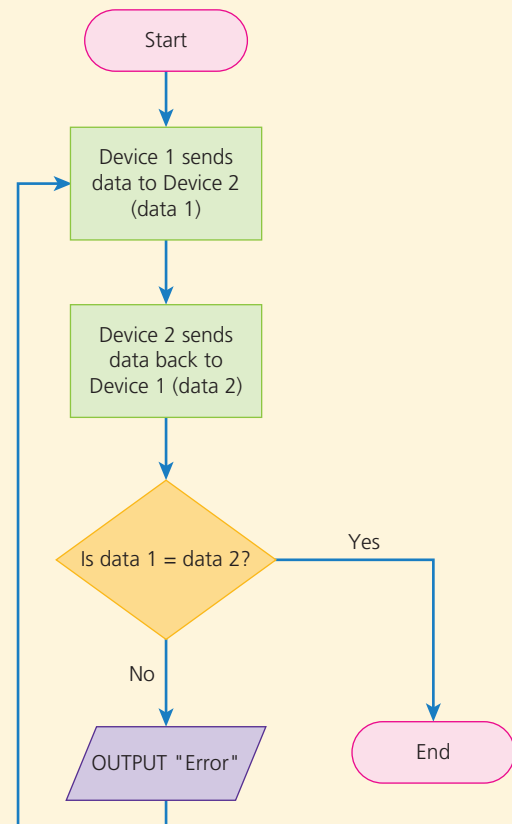
The sender then compares the two **sets** of data to check whether they match. If they match, there is no error. However, if they do not match, then the data is sent again.

The following **algorithm** shows a basic echo check.

For example, a computer transmits the binary number 00000001 (which represents **denary** 1). An error occurs causing 10000000 (denary 128) to be received. 10000000 is sent back to the first computer and the error is highlighted as the values do not match, so the original data is sent again.

Problems with echo checking

- Echo checking makes it impossible to tell whether the error occurred when the data was originally sent, or when it was returned to the sender.
- Echo checks mean that a lot more data is sent over a network.



KEYWORDS

binary: the number system that uses just two digits: 0 and 1; also known as 'base 2'

ASCII (American Standard Code for Information Interchange): a 7-bit binary code that represents all the keys on a standard keyboard

serial transmission: data is transferred one bit at a time

parallel transmission: 8 bits (or 1 byte) of data are transferred simultaneously

bit flip: when a single bit changes from 0 to 1, or 1 to 0, during transmission

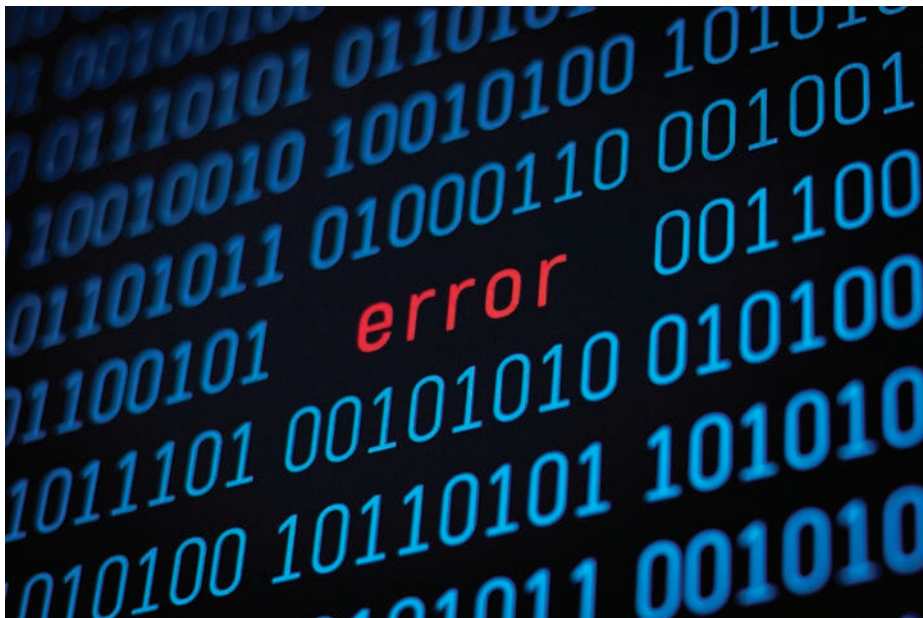
power surge: a temporary increase in power, often caused by lightning, which can damage computer hardware

data set: a collection of data items that are all related

algorithm: step-by-step instructions to solve a particular problem

denary format: a number system that uses the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 to represent every numerical value

Practise



Now that you understand how echo checks function, create a graphic-illustration comic to use as part of your youth group promotional materials.

- Provide at least six steps, including an illustration with a description for each step.
- Make your comic simple enough for somebody who is not familiar with echo checks to be able to follow the guidance and understand it.

Security concerns

Learn

You now know how echo checking can be used to help detect errors, but how do you know that the data that is being transmitted is secure? What are the threats to networks?

Hackers constantly try to gain **unauthorised** access to networks. There are a number of reasons for this, including to earn money illegally, to gather data (which is often also worth money) or to cause criminal damage.

There are four main types of threats: viruses, ransomware, spyware and unauthorised access.



Viruses

A virus is a computer program that is usually hidden within another **program** or file. It can replicate itself into other programs or files, which are then often passed between users/computers, or transmitted over networks. Viruses exist to cause harm, often damaging or deleting data without the owner's consent. Even small changes to a computer's **operating-system** files can be devastating to the system and cause it to malfunction.

One of the best-known viruses was the ILOVEYOU bug. In the year 2000, millions of people received the virus via email, with the subject line 'I love you'. When the recipient clicked and downloaded the file 'LOVE-LETTER-FOR-YOU.TXT.vbs', the virus was run. It overwrote important operating-system files and replicated itself multiple times. It is estimated to have cost users a total of \$15 billion in damages.

Ransomware

Ransomware is a type of software designed to block access to the files on a computer system until somebody pays a ransom.

Ransomware called 'WannaCry' targeted users of Windows operating systems and told them that they had to pay a fee, otherwise all their files would be encrypted and deleted, making them impossible to recover. This hit around 230,000 computers globally, including hospitals and doctors' surgeries.

Ooops, your files have been encrypted!



Your files will be lost

Time left:

59:59:59

Send \$600 worth of bitcoin to this address:
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Spyware

Spyware monitors the target computer's actions. For example, details of the keys that the user presses on the keyboard may be sent to the hacker. This means that the hacker could discover the keystrokes of passwords, giving them access to confidential login details.

A hacker often installs spyware on a computer or a network after they have gained unauthorised access. The software that the hacker installs cannot usually be detected and gives the hacker full control of and access to the computer system. They can also carry out this style of attack on mobile phones and tablets.

Unauthorised access

There are a number of ways in which hackers may try to gain access to computers and systems that they should not have access to.

● Social engineering

Hackers have developed ways of trying to find out as much information about somebody as possible in an attempt to guess their passwords. For example, if you met somebody and they asked you who your favourite sports team is, what month your birthday is in or what city you were born in, you would probably not consider this to be sinister. However, the hacker could use this information to try to guess your passwords.

Hackers may also try to use 'forgotten password' tools to answer secret questions that would give them the opportunity to reset a password.

● Cracking passwords

Brute-force attacks are a technique hackers use to try to gain access to computer systems or network devices. Hackers use very large 'dictionary' files that contain millions of words or known passphrases and they try every combination until they find the correct password. Hackers use computer programs that are able to try millions of different passwords every second to crack passwords automatically.

The most commonly used known passwords are often at the start of the dictionary files, and can be cracked very quickly.

Dictionary	How long to crack this password?	How many users have this password?
123456	Less than 1 second	Over 106 million
123456789	Less than 1 second	Over 46 million
12345	Less than 1 second	Over 32 million
qwerty	Less than 1 second	Over 22 million
password	Less than 1 second	Over 20 million

● Using information in an unauthorised way

People become hackers when they access networks that they are not allowed to. For example, if a company has sacked a member of staff and forgets to disable their user account, this person could still log into the company's systems and cause a threat to the network.

KEYWORDS

unauthorised: not allowed

program: the instructions that tell a computer system how to complete a task

operating system: the systems software that manages hardware and software, giving the user an interface to operate the computer

brute-force attack: a type of cyber-attack that uses a dictionary to try to discover passwords automatically

Practise

Use the internet to find out about famous **cyber-attacks**. Find an example for each of the following types of attack: **virus**, **spyware**, **unauthorised access** and **ransomware**. Find out the name of the cyber-attack, when it took place and what effect it had on the devices that were infected.

- 1 Create a mind map explaining what each type of cyber-attack is. This can be completed on paper or using any suitable software you have access to.
- 2 Find at least one appropriate example of each type of cyber-attack and add these to your mind map.



- 3 Try to find a cyber-attack that had an impact on a large number of people. Find the best example that you can and make a note of its name, what it did and the number of people it affected. Share your examples with the class to see who can find the cyber-attack that impacted the greatest number of people.

KEYWORD

cyber-attack: the collective name for all types of attacks on a computer or computer network

Deliver an exciting computing course for ages 11–14, building on students' existing computing skills and experience whilst demonstrating new concepts, with practice opportunities to ensure progression.

- Recap and activate students' prior knowledge with 'Do you remember?' panels and introduce more advanced skills with 'Challenge yourself!' tasks.
- Allow students to demonstrate their knowledge creatively with engaging end-of-unit projects that apply skills and concepts in a range of different contexts.
- Develop computational thinking with an emphasis on broadening understanding throughout the activities.
- Provide clear guidance on e-safety with a strong focus throughout.

For over 30 years we have been trusted by Cambridge schools around the world to provide quality support for teaching and learning. For this reason we have been selected by Cambridge Assessment International Education as an official publisher of endorsed material for their syllabuses.



This resource is endorsed by Cambridge Assessment International Education 

- ✓ Provides support as part of a set of resources for the Cambridge Lower Secondary Computing curriculum framework (0860) from 2021
- ✓ Has passed Cambridge International's rigorous quality-assurance process
- ✓ Developed by subject experts
- ✓ For Cambridge schools worldwide



Boost

This title is also available as an eBook with teacher support.

Visit hoddereducation.co.uk/boost to find out more.

Registered Cambridge International Schools benefit from high-quality programmes, assessments and a wide range of support so that teachers can effectively deliver Cambridge Lower Secondary.

Visit www.cambridgeinternational.org/lowersecondary to find out more.