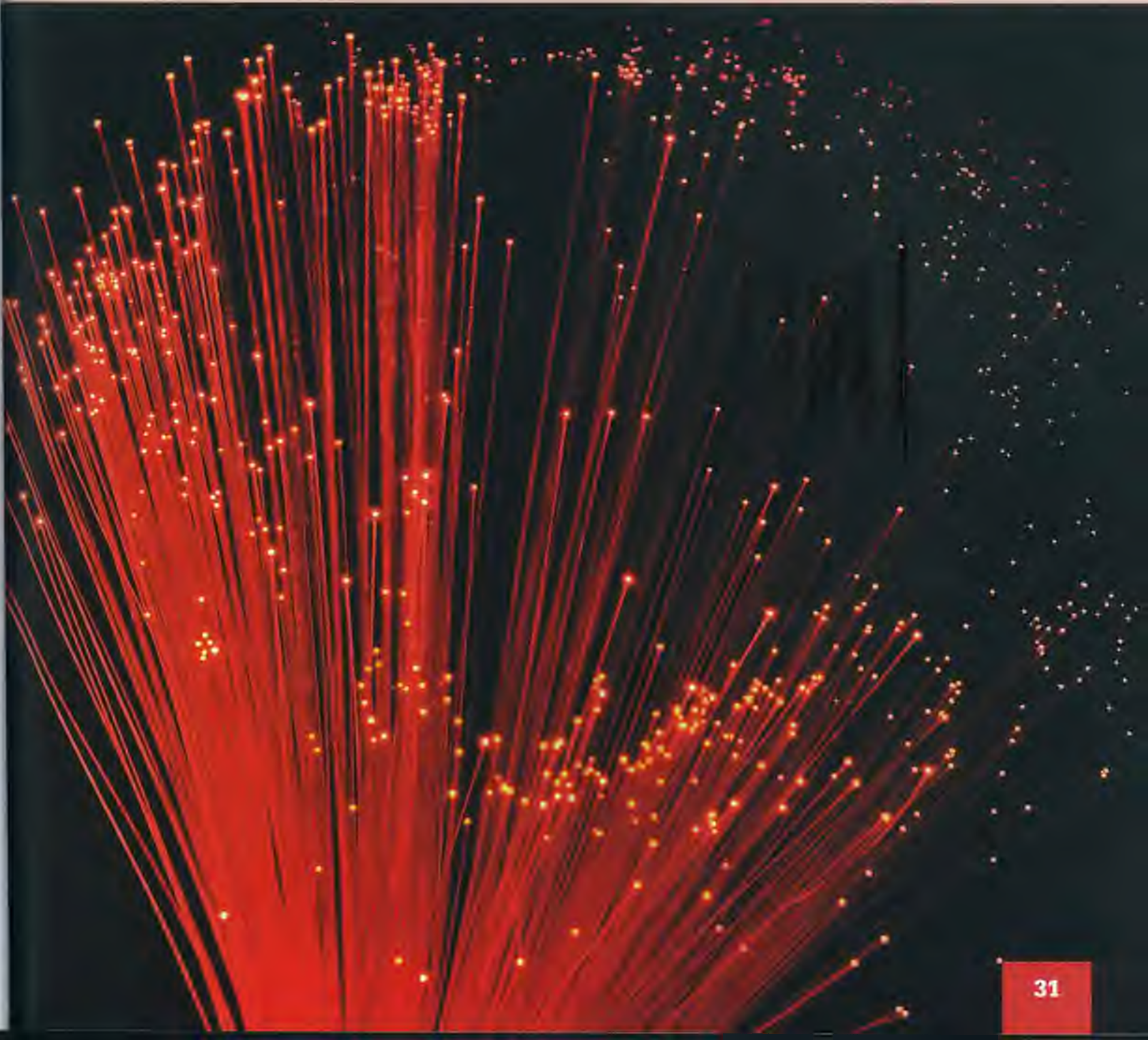
2 Communications and the Internet



Syllabus reference

1.2.1 Data transmission

Learners should be able to: show understanding of what is meant by transmission of data; distinguish between simplex, duplex and half-duplex data transmission; show understanding of the need to check for errors.

See also:

1.1 Binary systems (Bits and bytes)

2.1 Data transmission

How data is transmitted

Introduction

In Chapter 1 you learned how data is held in a digital electronic format inside a computer. In this chapter you will learn how data is shared and communicated between computers.

Data transmission

Computers hold data in binary form, using on/off switches. Each on/off signal represents one bit of data. Computers can turn this binary data into a stream of on/off signals which can be transmitted. That means the signals are sent from one place to another. The signals can be:

- electrical pulses that travel down metal cables
- pulses of light that travel down a fibre-optic cable
- wireless signals – radio signals, microwave and infrared waves – when the bits are sent as electromagnetic waves that move through space, and also air and many other materials (including human beings, who are not affected by them).

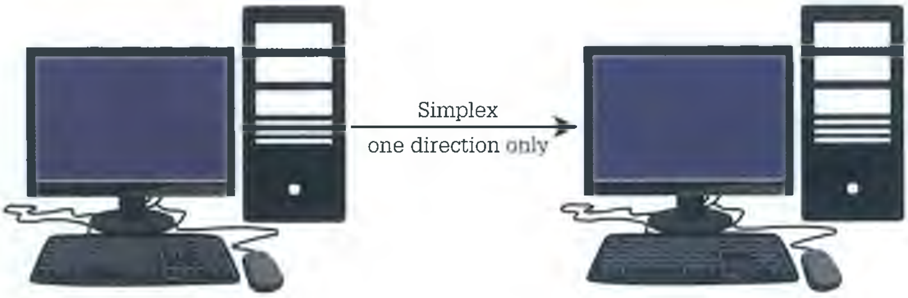
Whatever system is used to carry the on/off signals, it is known as the transmission medium.

Long or short distance

Data transmission is used to link computers. The computers can share and send data. The Internet is based on long-distance communication links.

Data transmission is also used over short distances. The different parts of a computer transmit data to each other. When you send your work to a printer, that requires data transmission.

Bluetooth is an example of a short distance wireless data link. Bluetooth can be used to link an earpiece (headset) to a mobile phone.



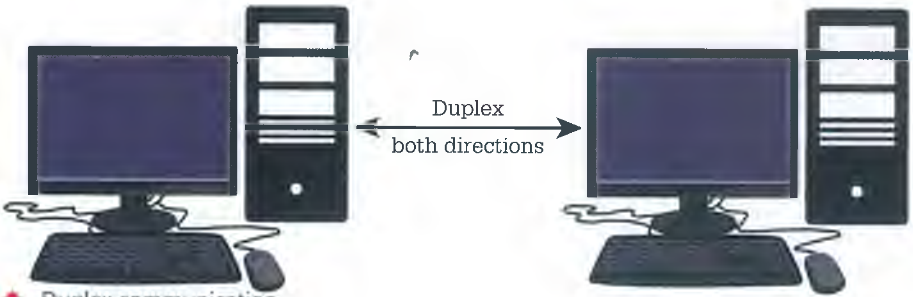
Simplex communication

Simplex and duplex

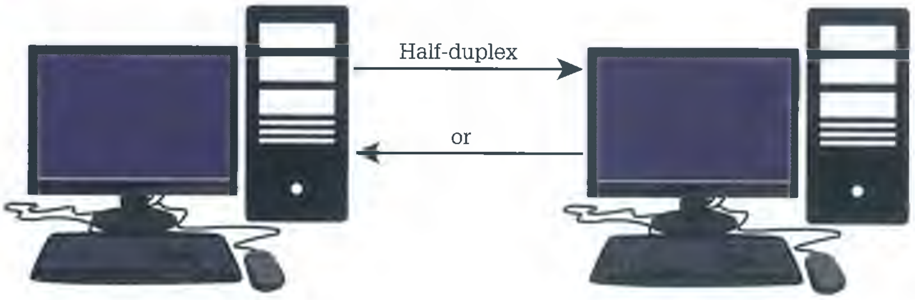
Communication links can be simplex, duplex or half-duplex.

- Simplex communication is a one-way link. The signal can only go in one direction. An example of a simplex communication is the signal from a closed-circuit TV camera to a security guard's monitor. The security guard can see on the monitor what the camera sends, but cannot send anything back to the camera.

- Duplex communication is a two-way link. The signal can go both ways. A phone conversation is an example of duplex communication. Both people can talk. Both people can listen.
- Half-duplex means the link can only carry signals in one direction at a time. The two sides have to take turns to send a signal. A walkie-talkie system is half-duplex.



Duplex communication



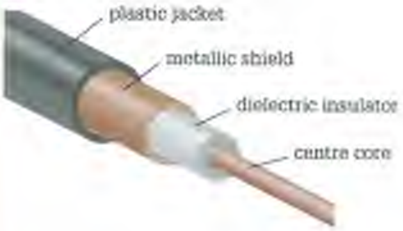
Half-duplex communication

Types of cable

Cables connect devices together. Signals are sent along the cable. These are the main types of cable:

- Twisted pair cable: this is made of pairs of copper wires, individually insulated then twisted together. It is inexpensive, flexible and convenient, but it is not suitable for a long-distance link. Electrical interference can cause errors in the data. It is used for short-distance links.
- Coaxial cable: this is a metal cable, surrounded by a layer of insulation then another layer of metal. It is protected against electrical interference. It is more expensive than twisted pair, and it is not as flexible. It is used where cables need to go close to electrical and radio equipment.
- Fibre-optic cable is fairly expensive but it has many advantages over the other types of cable. It is not affected by electrical interference. It is suitable for long-distance links.

Twisted pair cable



Coaxial cable

Fibre-optic cable

Test yourself

1. What is the alternative to using cables for data transmission?
2. What is the difference between the content of a transmission and the transmission medium?
3. A computer is not connected to the Internet or any other computer. However, it still uses data transmission. Explain why.
4. I have a radio receiver but not a transmitter. What type of communication link is this?
5. Draw a diagram to show the difference between simplex, duplex and half-duplex communication.

Learning activities

You have seen that wireless communication can use different forms of signal: radio, microwave and infrared. Investigate examples of each type of wireless signal being used for communication.

Find examples of how the three types of cable are used.

Syllabus reference

1.2.1 Data transmission

Learners should be able to: show understanding of what is meant by transmission of data; distinguish between serial and parallel data transmission; show understanding of the reasons for choosing serial or parallel data transmission.

See also:

Chapter 1 Data representation

Serial or parallel?

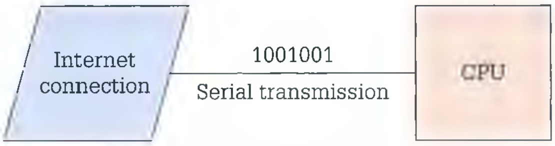
Introduction

You have learned that data transmission happens when bits are turned into signals. The signals are sent from one place to another. Now you will learn about the types of data transmission.

Serial transmission

Most data transmission is serial transmission. In serial transmission, the bits that make up the data are sent one at a time. The bits all travel along the same transmission medium, one after the other, in a series. The signals are sent down a single wire, or as a wireless signal. The bits arrive at the other end one at a time.

Serial transmission is the most reliable method of data transmission. The bits are kept separate from each other. They arrive in the same order that they were sent. Serial transmission is used for long-distance communication, for example an Internet connection.

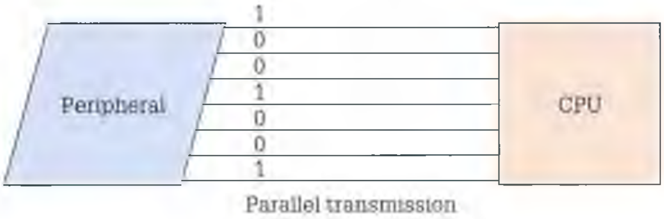


↑ Serial transmission – the eight bits are sent one after the other down the same wire

Parallel transmission

You have learned that bits are held in groups of eight called bytes.

Some communication links use several wires at the same time. Each wire carries one bit, so several bits can be sent at the same time. Some parallel systems have eight wires. This means that all the bits in a byte can be sent at once. Each bit goes down a different wire. All the bits arrive at the same time.



↑ Parallel transmission – the eight bits are sent at the same time along different wires

Advantages and disadvantages

Parallel transmission is quicker than serial transmission. Several bits are transmitted at the same time, so it takes less time to send the data.

However, there are risks when you use parallel transmission. There is more chance of an error in the signal. Microscopic differences in the wires might mean that they transmit signals at slightly different speeds. Over a long distance that might turn into a big difference. The bits won't all arrive at the same time. The signal will not be transmitted accurately. For this reason, parallel transmission is only used for short-distance communications, for example to connect a monitor to the computer.

Serial transmission can take longer, because the bits are sent one at a time, but it is more reliable over a long distance.

Long or short distance?

Some connections are long distance. For example, Internet connections link computers all over the world. For these connections we would use serial transmission. Some connections are very short distance, for example connections between components inside the computer. For these, we might use parallel transmission.

Other connections are between these extremes, for example the connection between a computer and a printer in the same room. In this case either serial or parallel transmission can be chosen.

Serial and parallel ports

Old personal computers used to be equipped with both serial ports and parallel ports, and you could see the difference between them by looking at the pins on their connectors.

A serial port used only a few pins, with just one reserved for transmitting data and another for receiving. Other pins might be used to control the port, but they weren't used for data.

A serial port

A parallel port

Test yourself

1. What is the main advantage of parallel transmission?

2. Explain why parallel transmission may not be reliable over long distances.

3. What is the visual difference between serial and parallel cable?

4. What is a port on a computer?

Learning activity

Use graphics software to draw a diagram showing both serial and parallel transmission.

Complete this table to show the advantages and disadvantages of the different types of transmission

	Advantages	Disadvantages	Uses
Serial			Long distance
Parallel			Short distance

Syllabus reference

1.2.1 Data transmission

Learners should be able to: show understanding of the use of serial and parallel data transmission, in universal serial bus (USB) and integrated circuit (IC).

See also:

3.3 Inside the CPU

The lines on the circuit board are actually thin copper wires acting as data buses

Data bus

Introduction

You have learned about data transmission between computers. In this section you will learn about data transmission within a single computer system. This is how the different parts of a computer "talk to" each other.

Integrated circuits

Data in the computer is stored using on/off electronic switches. An integrated circuit (IC) is a collection of microscopic electronic circuits, sealed into a single plastic or ceramic package. Different ICs are used for different tasks inside the computer. Many ICs are used for data storage. One of the ICs, the central processing unit (CPU), contains the computer's processor and registers. All these parts must be connected together. We will talk more about the CPU in *3.3 Inside the CPU*.

The different ICs are linked by wired connections called data buses. Some ICs, particularly CPUs, have internal buses too, made from metallic layers within the IC. Each part of the IC works very quickly. The speed of a whole computer is strongly affected by how quickly the buses can transmit data between the different parts.

Parallel data bus

The buses inside the CPU, and between CPU and RAM, use parallel transmission, which has advantages and disadvantages:

- The advantage of parallel transmission is speed. The speed of each data bus strongly affects the performance of the computer system.
- The disadvantage of parallel transmission is that it needs more wires, so it takes up more of the very limited space available inside the IC or on the circuit board.

Connecting peripherals

The processor is at the centre of the computer. That is where the work of the computer takes place. A computer needs other devices such as a screen, a keyboard and a mouse. These additional devices are called peripherals. The peripherals have to be connected to the processor. Buses are used to connect the peripherals to the processor.

There are several ways to join a peripheral to the processor. It can be done using:

- permanent wiring, for example the keyboard of a laptop is permanently wired into the computer casing
- a plug-in cable, for example a monitor can be plugged in to the computer
- a wireless connection, for example a wireless mouse.

In each case, a bus is needed to complete the connection.

Syllabus reference

1.1.3 Data representation

Learners should be able to identify and describe methods of error detection and correction, such as automatic repeat request (ARQ).

Transmission errors

Introduction

Data transmission means sending bits and bytes from one location to another. It is important that the data is transmitted in full and without errors. In the rest of this chapter you will learn about ways to detect errors.

Transmission errors

Data is transmitted through a medium, which may use a cabled or a wireless connection. The transmission media carries bits in the form of electrical, radio or optical (light) pulses. All types of transmission media can be affected by errors.

Errors can be caused by flaws in the transmission medium, such as imperfections in a copper wire. Errors can be caused by external factors, such as electrical fields. We can design systems to reduce errors. For example, wires can be shielded by an outer conductive layer, to prevent electrical interference. Despite this, errors can still occur.

Transmission errors can have serious effects. Every bit in a signal is important. Changing one bit alters the value of the binary number. The whole signal will be wrong. For this reason it is important to check for errors in transmitted data. If the data has an error, it can be sent again.

Types of error

Errors in transmission can mean that:

- some of the bits are lost from the data stream
- extra bits are added to the data stream
- 1 bits change to 0, or 0 bits change to 1.

If a human operator is involved, for example someone typing the data, the person can also make errors. An error made in copying data, for example when typing it, is called a transcription error. An error where two letters or numbers are in the wrong order is called a transposition error.

Transmitter and receiver

Data transmission involves a transmitter and a receiver.

- The transmitter is the device that has the data to start with, and sends it.
- The receiver is the device that gets the data, after transmission.

Typically these devices are computers, but they could be a computer and its peripherals. The receiver will check the accuracy of the data sent by the transmitter. If an error is found, the receiver will ask the transmitter to send the data again.

Ways to detect errors

On the next few pages you will learn about ways the computer can check a transmission for errors. Parity checks are discussed on pages 40–41. Check digits are discussed on pages 42–43.

Automatic Repeat reQuest (ARQ)

The error checks methods are used in a process called automatic repeat request (ARQ). This is a method to ensure correct transmission of data. It works like this:

- The transmitter sends some data (called a packet).
- When the receiver gets the data packet, it checks it for errors.
- If the receiver finds no errors, it will send an acknowledgement.
- If the transmitter doesn't receive an acknowledgement, it sends the data again.

The transmitter will keep on sending the data packet until it receives an acknowledgement. There is usually a time limit. Once the time is up, the transmitter will stop trying to send the package. The signal has timed out.

Test yourself

1. Give the meanings of transmission errors, transposition errors and transcription errors.
2. What changes can occur to data bits as the result of transmission errors?
3. How does shielding help to prevent transmission errors?
4. Explain the roles of the transmitter and receiver devices in the ARQ process.

Types of error

If two digits or letters are accidentally swapped around, this is called a **transposition error**. It is one of the most common types of **transmission error**.

Syllabus reference

1.2.1 Data transmission

Learners should be able to explain how parity bits are used for error detection.

1.1.3 Data representation

Learners should be able to identify and describe methods of error detection and correction, such as parity checks.

Parity check

Introduction

You have learned that it is important to detect errors in data transmission. In this section you will learn about parity checks. A parity check is one way to check data for errors. Make sure you know the difference between the role of receiver and transmitter.

Parity

"Parity" is a term from mathematics. It means whether a number is odd or even. Parity is used to check whether data has errors in it. The most common type of parity check is known as an even parity bit.

Before the data is sent, the transmitter counts how many 1s there are in each byte. The transmitter then adds an extra bit to the end of each byte:

- If there is an even number of 1s in the byte, the parity bit is set to 0.
- If there is an odd number of 1s in the byte, the parity bit is set to 1.

This extra bit makes sure the number of 1s transmitted is an even number.

After the data is received:

- The receiver counts how many 1s there are in each byte plus its parity bit.
- Each byte plus parity bit should have an even number of 1s.

If any of the bytes with its parity bit has an odd number of bits, the receiver will know there was an error during transmission. The data must be sent again.

Even parity bit

In the example on this page, the even parity bit is shown at the right of the transmitted number. In practice it may not be stored in this location.

Worked example

The transmitter got ready to send this signal.

0	1	1	0	0	0	1	

There are three 1s in the data. That is an odd number, so the parity bit was set to 1. Now there are four 1s in the byte – an even number. The parity bit is highlighted.

0	1	1	0	0	0	1	1

Next the signal was transmitted. There was an error during transmission. One of the bits was altered by an error in transmission. The error is highlighted. The signal has gone wrong.

0	1	0	0	0	0	1	1

The computer that received the data added up the number of 1s in the signal. There were three 1s in the signal. That is an odd number, so there must have been a transmission error.

In conclusion: the error has been spotted. The data has to be sent again.

Odd parity

Some communication systems use “odd parity”. In this system the number of 1s in each byte is an odd number. Otherwise it works just the same as even parity. Of course, the transmitter and receiver must both use the same system.

Which bit?

Data is normally stored and sent in groups of eight bits:

- In some cases, seven of the bits are used to send the data. The eighth bit is a parity bit. The parity bit is part of the byte.
- In other cases all eight bits are used to send the data. The parity bit is sent as an extra signal following the byte.

Limitations

The parity method is not perfect:

- If there are two errors in a byte (or any even number of errors) then the parity check will fail.
- If two bits get swapped round (transposition error) then the parity check will not spot the error.

For this reason other data checks are used as well as a parity bit.

Test yourself

Here is a block of data to be transmitted.

0 0 0 1 1 0 0

1 1 1 0 1 1 0

1 0 1 0 1 0 0

1 1 1 1 0 0 0

1 0 0 0 1 1 0

1 0 0 1 1 1 0

0 0 0 1 0 0 1

Assume that you are using even parity and add a parity bit to each row.

Learning activity

This is an extension activity. You will work with the block of data from the last question. You have added an even parity bit in each row. Now look at each column of data. Assume that you are using even parity and add a parity bit to the bottom of each column.

Now the data has a parity bit at the end of each row and the bottom of each column. This gives an additional check. It overcomes the two limitations mentioned on this page.

Syllabus reference

1.2.1 Data transmission

Learners should be able to identify and describe methods of error detection and correction, such as check digits and checksums.

Check digit and checksum

Introduction

Parity checks are error checks for binary data. In this section you will learn about error checks that can be used for denary numbers. These checks can detect transmission errors, and human errors such as typing (transcription) errors.

Check digit

A check digit is similar to a parity bit. It is added to the end of a denary number. The check digit is worked out from the digits in the number.

A check digit is used in the same way as a parity bit:

- A computer works out the check digit before transmission, and sends it with the number.
- The receiving computer works out the check digit after transmission, and compares it to the original.
- The two check digits should match.
- If they do not match there has been an error in transmitting the number.

Calculate the check digit

There is more than one way to work out the check digit from a denary number.

Simple method

This is the simplest way to work out the check digit:

- Add up all the digits in the number to give the sum of the digits.
- Divide the sum by 10.
- The remainder from this division is used as the check digit.

The remainder when dividing a value by 10 is called the value modulo 10, or the value mod 10. Sometimes a check digit uses modulo 11, where the sum is divided by 11. If the remainder is 10, the letter X is used as the check digit.

A simple check digit cannot identify a transposition error. That is when two digits get swapped around. That is because a transposition of two digits will not change the overall sum of the digits.

Sum

In mathematics the sum is the result of adding together a group of numbers.

Modulo (mod)

In mathematics the modulo is the remainder that is left after a division has been carried out. It is shortened to "mod".

Other methods

For this reason, other ways to calculate a check digit have been invented. The digits in different positions in the number are multiplied by different values. Then the numbers are added together and the check digit is calculated in one of the following ways:

- using the Luhn method, every second digit is multiplied by 2 and the total must be an exact multiple of 10.
- using the ISBN-10 method, every digit is multiplied by its position in the number: the first digit by 1, the next by 2 and so on. The check digit is the total mod11.

These methods are more complex, but they have a big advantage. If a digit is accidentally transmitted in the wrong position, the sum will change. The check digit will change. That means these methods will detect transposition errors.

Every credit card has a number on it which includes a check digit

Checksum

Using a checksum is a way of checking a group of numbers:

- The transmitter adds up the total of a group of numbers before transmission.
- The transmitter sends the total along with the numbers.
- The receiver works out the total and compares it to the transmitted total.
- The two totals should match. If the two totals do not match then there has been an error. The data must be sent again.

You can use a checksum even if the sum value does not represent a real total. For example, you can use a checksum when sending a group of phone numbers. A number of this kind – which is not a real total – is called a hash total.

Test yourself

1. A check digit is calculated twice, once each by two different computers. Explain why.
2. What is 32 mod 10?
3. Why is any value mod 10 always a single-digit number?
4. What is the limitation with using a simple sum and mod 10 check digit?
5. When do we call a control sum a hash total?

Learning activity

1. Write down your phone number. Calculate a simple check digit for your phone number, using mod 10.
2. Collect the phone numbers of five friends. Calculate a checksum for this list of numbers.
3. Find a book with a 10-digit ISBN code. Using the first 9 digits, work out the check digit. Check this against the example you see on the real book. It should match.

Use of check digits

A credit card number includes a check digit. Since 1960, the Luhn method has been used to calculate check digits on credit cards.

Every book published is given a code number called the International Standard Book Number (ISBN). These numbers can be either 10 or 13 digits long (ISBN-10 or ISBN-13). Both formats include check digits.

Syllabus reference

1.2.3 Internet principles of operation

Learners should be able to show understanding of the role of an Internet service provider (ISP).

See also:

2.3 Safety online

2.2 The Internet

What is the Internet?

Introduction

You have learned about data transmission. Data transmission allows computers to send and share data. A group of computers linked together in this way is called a network. The Internet is the biggest network in the world. In this section you will learn about the Internet.

The Internet

Connected computers can share data through data transmission links. The Internet is a system of computer connections that covers the whole world. To be connected to the Internet a computer must have:

- a data transmission connection (wired or wireless)
- Internet software
- shared protocols.

Any computer can be connected to the Internet if it has these. There were very few computers with an Internet connection 20 or 30 years ago. Now there are literally billions of computers and other devices connected to the Internet. The Internet grows bigger every day. About half the people on Earth have used the Internet.

Nobody is in charge of the Internet. The Internet is the system of links that people can use to share data. Nobody checks that the data is correct. Nobody can control what is on the Internet.

The Internet can be very useful and helpful, but it can also have risks and problems. Learn more about risks and how to keep safe in 2.3 *Safety online*.

An illustration of the connections that make the Internet

Internet service provider (ISP)

You can buy a computer that can connect to the Internet. What does it connect to, though?

Most people are connected to the Internet by an Internet Service Provider (ISP). An ISP is an organisation that enables people to use the Internet. Many ISPs are commercial companies that offer Internet services for a connection fee.

The services that might be offered by an ISP include:

- sending signals between the Internet and your computer
- providing email services
- hosting a web page for you.

Different ISPs use different ways of connecting computers to the Internet. Some use the public phone lines; some use wireless, or cables.

Internet software

"Software" means the instructions that let your computer carry out actions. Several different types of software can be used to connect to the Internet. This software reads the signals that come via the Internet connection. It turns these signals into a form that you can see and use on your computer. It also converts the signals from your computer into a suitable form. For example, if you type a message, the software converts your text into a form that can be sent over the Internet and be understood by other computers.

The most common Internet software is a web browser. You will find out more about web browsers on page 47.

Shared protocols

Protocols are communication standards. They are standard rules about how data is turned into signals. If two computers share data, they must use the same protocols. All computers that connect to the Internet use the same protocols.

Key protocols of the Internet are TCP and IP (see pages 52–53).

Test yourself

1. Many ISPs are commercial companies. How do these companies make money?
2. As well as giving you an Internet connection, what other services might an ISP provide?
3. Who makes sure that there are no mistakes on the Internet?
4. As well as a wired or wireless connection, what else do you need to use the Internet?

Learning activity

Use online research to find out how many computers are connected to the Internet. If you find the answer on a website, or in a book, check the date that it was published. The answer is changing all the time.

Not the World Wide Web

The Internet is not the same as the World Wide Web. Find out the difference on page 46.

What is the World Wide Web?

Syllabus reference

1.2.3 Internet principles of operation

Learners should be able to show understanding of the role of the browser.

Introduction

You have learned that the Internet is a series of connections and standards. Many different services and features are available through Internet connections. The most popular is the World Wide Web. In this section you will learn what the World Wide Web is.

Website

The World Wide Web (also called the Web) is the collection of all the web pages in the world. The World Wide Web is the most popular service available through an Internet connection.

A web page is a multimedia document that you can read over the Internet. “Multimedia” means a document that can include many different types of data: text, images, sound and video. Web pages are created in a format called HTML. Find out more about HTML on pages 48–49. Web pages can be viewed by software called a web browser.

Wikipedia has been viewed by hundreds of millions of users

A website is a collection of web pages, stored on a web server. Anybody with an Internet connection can connect to the website and look at the web pages.

Some popular sites include:

- Google
- Amazon
- Twitter
- Facebook
- Wikipedia
- Youtube

Web server

A web server is a computer that is permanently connected to the Internet. A web server hosts web pages, which means that the web server holds the content of the web page in its storage. A web server will send the contents of the web page along an Internet connection to another computer. The web page can be viewed by Internet users. Many ISPs offer web hosting as one of their services.

Web addresses

Every web server has its own numeric address, called an IP address, and a number of text-based names. Every website and web page hosted by the server has its own name, called a URL. The URL contains one of the web server's names. You will learn more about IP addresses and URLs on pages 52–53.

Web browser

A web browser is software that lets you look at web pages. To connect to a web page you type its URL into your web browser. The web browser will:

- get the web server's name from the URL, and use that to connect to the web server
- transfer a copy of the web page onto your computer
- display the web page so that you can interact with the content.

Web pages are written in a format called HTML. A web browser can read HTML. It will interpret the content and show it on your screen.

There are several popular web browsers, including:

- Internet Explorer
- Firefox
- Chrome.

Different browsers may display web pages slightly differently.

⬆ Google Chrome is one of the most widely used web browsers

Web protocols

The use of web pages depends on shared protocols:

- HTTP is the protocol that allows web pages to be shared. Find out more about HTTP on pages 50–51.
- IP is the protocol that gives every web server an address. Find out more about IP on pages 52–53.

Test yourself

1. What is the difference between a website and a web page?
2. What types of data can you find on a web page?
3. Many ISPs offer a web hosting service. What does that mean?
4. Describe the job of a web browser.

Learning activity

Choose one of the popular websites listed on the previous page.

Write a short report on the website you have chosen. What features does it have? Why is it so popular?

Download

When you download web content, you copy it from a web server onto your own computer. That means you can see and use the web content on your own computer.

Upload

When you upload web content, you copy it from your computer onto a web server. That means other computers can access it. You have made the content available to other people.

HTML

Syllabus reference

1.2.3 Internet principles of operation

Learners should be able to: show understanding of what is meant by HTML; distinguish between HTML structure and presentation.

Introduction

You have learned that the Web is made of all the web pages in the world. Web pages are made using HTML, which stands for "hypertext markup language". In this section you will learn about HTML.

Markup

HTML is a markup language. A markup language is used to add descriptions to pieces of text in a document. The descriptions are called tags. HTML tags tell a web browser how to display a document. When you make a web page you must enter the text, and also the HTML tags that tell the computer how to display the text.

Tags

Tags generally come in pairs. One tag turns a feature on, another tag turns it off. For example, the tag <h1> turns on the main heading style. The tag </h1> turns it off.

A web page may include the text "My Family". With HTML tags it may look like this:

```
<h1>My Family</h1>
```

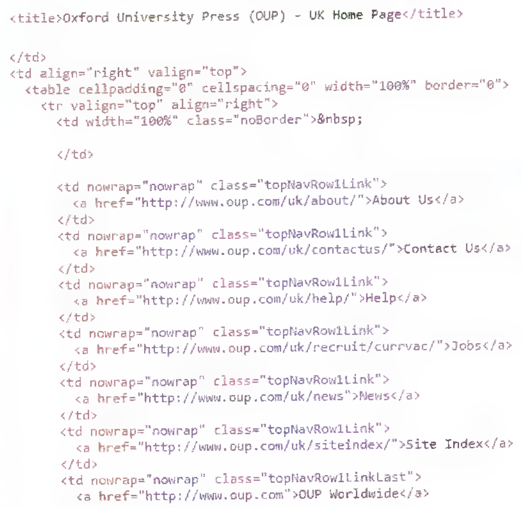
When you open the web page in a browser you will not see those tags. The browser will display the words "My Family" as a large heading.

Example

Here is part of the HTML that defines the main (or home) web page of the OUP website: the publishers of the book you are reading.

As you can see, there are a lot of HTML tags. This is only a small part of the HTML that defines the page.

When your browser displays the same page it looks like this.



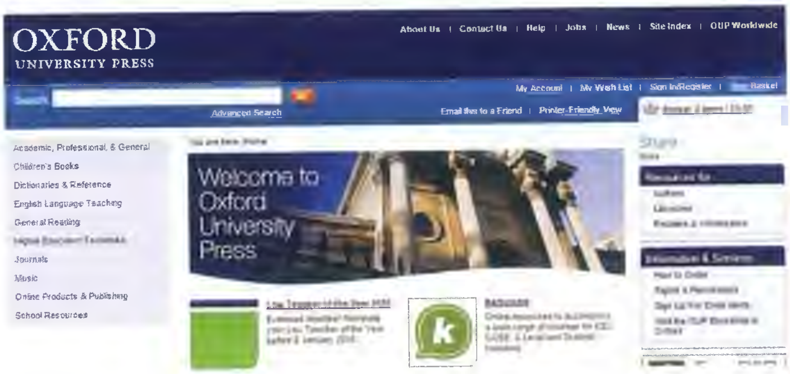
```
<title>Oxford University Press (OUP) - UK Home Page</title>

</td>
<td align="right" valign="top">
  <table cellpadding="0" cellspacing="0" width="100%" border="0">
    <tr valign="top" align="right">
      <td width="100%" class="noBorder">&nbsp;

      </td>

      <td nowrap="nowrap" class="topNavRow1Link">
        <a href="http://www.oup.com/uk/about/">About Us</a>
      </td>
      <td nowrap="nowrap" class="topNavRow1Link">
        <a href="http://www.oup.com/uk/contactus/">Contact Us</a>
      </td>
      <td nowrap="nowrap" class="topNavRow1Link">
        <a href="http://www.oup.com/uk/help/">Help</a>
      </td>
      <td nowrap="nowrap" class="topNavRow1Link">
        <a href="http://www.oup.com/uk/recruit/currvac/">Jobs</a>
      </td>
      <td nowrap="nowrap" class="topNavRow1Link">
        <a href="http://www.oup.com/uk/news">News</a>
      </td>
      <td nowrap="nowrap" class="topNavRow1Link">
        <a href="http://www.oup.com/uk/siteindex/">Site Index</a>
      </td>
      <td nowrap="nowrap" class="topNavRow1LinkLast">
        <a href="http://www.oup.com">OUP Worldwide</a>
```

This HTML defines the OUP home web page


OXFORD
UNIVERSITY PRESS
About Us | Contact Us | Help | Jobs | News | Site Index | OUP Worldwide
My Account | My Wish List | Sign In/Register | Basket
Search
Advanced Search
Email this to a Friend | Printer-Friendly View
Academic, Professional, & General
Children's Books
Dictionaries & Reference
English Language Teaching
General Reading
Journals
Music
Online Products & Publishing
School Resources
Welcome to Oxford University Press

When the HTML is displayed by your browser it looks like this

Your web browser software reads the HTML, and displays this web page.

Structure and presentation

HTML tags tell the web browser how to display the web page. There are two main types of HTML tag. They have different effects:

- **Structure:** Some HTML tags control the layout of the web page. This includes adding a page title, headings, sections and paragraphs. For example, the tags `<h1></h1>` mark the start and end of a heading.
- **Presentation:** Some HTML tags change how the web page is displayed. For example the tags `<b></b>` mark the start and end of bold text.

You can also change presentation by adding "style" instructions to HTML. For example this command sets the colours for a whole web page:

```
<style>
body {background-color:yellow;}
h1   {color:red;}
p    {color:green;}
</style>
```

Can you work out what this page would look like? Do you think these are good colour choices?

You can store style commands in an external file called a "Cascading Style Sheet" (CSS). You can link lots of different web pages to the CSS file. All the web pages will have the same style. If you make a change to the CSS file, all the pages will change. This gives a consistent, professional feel to your work.

Hypertext

HTML means "hypertext markup language" – but what is hypertext?

Hypertext is text that makes a link to a new web page. Most web pages include hypertext. Hypertext links are often shown on the screen as blue, underlined text. When you click on a hypertext link your web browser will connect to the linked page. It will be displayed in your browser. In this way you can browse, moving from one website to another.

You have learned that HTML makes hypertext links. Links can be connected to images or areas of the screen as well as to text.

How to make a website

A web hosting service will help you to make a website. The pages of your site will be stored on their web server. That is called publishing your website. The pages can be seen by anyone with an Internet connection.

A web hosting service will provide software to help you make the web pages. The software makes it easy to design the web page. You do not need to type HTML tags. You choose features such as text colour and size from menus. The software turns your choices into HTML. It is similar to using a word processor to make an ordinary document.

Learning activities

1. Connect to a website with your browser. Right-click on the web page and pick "View page source" from the menu. You will see the HTML that made the page you are looking at.
2. Work in a group or as a whole class. Use a free online web hosting service. Create a web page about what you have learned so far in iGCSE Computer Science.

Test yourself

1. HTML stands for "hypertext markup language". Explain the meaning of "hypertext" and "markup".
2. HTML tags often come in pairs. Why?
3. A student made a website. She did not know HTML. How did she manage to make the site?
4. When you look at a website in your browser you do not see the HTML tags. Why?

Syllabus reference

1.2.3 Internet principles of operation

Learners should be able to: show understanding of what is meant by hypertext transfer protocol (HTTP and HTTPS); show understanding of what is meant by cookies.

See also:

6.2 Security protection

HTTP: Hypertext transfer protocol

Introduction

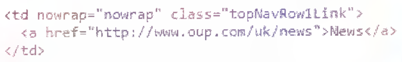
You have learned that hyperlinks are a key feature of web pages. Hypertext transfer protocol (shortened to "HTTP") is the protocol that makes hyperlinks work. In this section you will learn about HTTP.

Hyperlinks

A key feature of a web page is that it can include links (also called hyperlinks). A link is a piece of text on the page, or an image such as button. When you click on the link your browser connects to a new page and displays it in your browser. The hyperlink could take you to different part of the same website, or a new site.

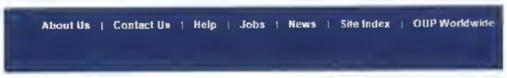
Example

On the previous page you saw part of the HTML that defines the OUP website. The OUP website includes the following HTML. This HTML makes the text "News" into a hyperlink.



```
<td nowrap="nowrap" class="topNavRow1Link">
  <a href="http://www.oup.com/uk/news">News</a>
</td>
```

⬆ This HTML defines the word "News" as a hyperlink


About Us | Contact Us | Help | Jobs | News | Site Index | OUP Worldwide

⬆ The word "News" on this menu bar is a link

The HTML makes a hyperlink to the following web address:

http://www.oup.com/uk/news

The HTML displays the following link on the OUP page.

If you click on the word "News" on the OUP website, your web browser will connect to the web address shown above.

HTTP

HTTP is the protocol that makes hyperlinks work.

A protocol is a shared standard for communication. All web servers use the HTTP protocol. All web browsers use the HTTP protocol too. That is why links work on every web page, and with every browser. Without HTTP the World Wide Web would not work.

The address of every web page begins http:// or https:// That shows you that the page uses the HTTP protocol. Find out more about web addresses on pages 52–53.

HTTPS

HTTPS stands for "HTTP secure". HTTPS is an extended protocol. It has extra features: authentication and encryption. These are not part of the basic HTTP protocol.

Authentication

Some websites are fake. They look as if they are run by a well-known company, such as a bank, but they are not. Learn more about fake websites on page 55.

"Authentic" means not fake. Authenticating a website means checking that it is not fake. HTTPS authenticates a website. If a web page's URL begins with https, you can be sure it is not fake. Learn more about security protocols in *6.2 Security protection (Security protocols)*.

Encryption

When you are using a website you often type details such as your name and address. These details are sent to the website.

Encryption means putting data into a secret code. HTTPS encrypts everything you send to a website, so that nobody can see what you are sending there. This makes it safer to send data to the website. Learn more about encryption in *6.2 Security protection (Encryption)*.

Cookies

Websites often need data that relates specifically to you, for example your email account or bank account details. HTTP and HTTPS do not transmit user details, so when you go back to a website using HTTP protocol, it does not know who you are.

Websites get round this problem by using HTTP "cookies". When you use a website, it collects key data about what you do there. This data is packaged up as a small binary file called a cookie. The binary file is sent back to your computer. It is stored on your own computer, not on the website.

Next time you use the website, the cookie goes from your web browser to the site. The cookie tells the website key facts about you, for example what you bought last time.

Some people do not like cookies, because of privacy concerns. However, cookies are in very common use.

Q

Test yourself

1. What key feature of every web page is supported by HTTP?
2. What is authentication? Explain how authentication makes it safer for you to use the Internet.
3. What is encryption? Explain how encryption makes it safer for you to use the Internet.
4. Explain what a cookie is. What are the advantages and disadvantages of cookies?

Q

Learning activity

In the previous section your class created a web page. Expand the content by including a selection of links to useful websites.

Syllabus reference

1.2.3 Internet principles of operation

Learners should be able to: show understanding of the concepts of MAC address, Internet protocol (IP) address, uniform resource locator (URL).

See also:

6.2 Security protection (Security protocols)

TCP/IP

Introduction

You have learned that a protocol is a standard for communication. In this section you will learn about the main protocol system that allows the Internet to work.

Internet protocols

The main protocol system of the Internet is called TCP/IP:

- TCP stands for "Transmission Control Protocol". This protocol controls the way data packets are transmitted along Internet connections.
- IP stands for "Internet Protocol". This protocol makes sure the data packets go to the right place. Every location on the Internet has an IP address. IP sends the data to the right address.

IP address

An IP address is a number given to every device that is connected to the Internet. Every device has a different number. The IP address identifies the device. The IP address is used to find a route across the Internet to the device's local area network. This means data can be sent to the device down the route.

You have learned that numbers can be stored as binary digits (bits). The larger the number the more bits are needed. IP addresses are very large numbers: 128 bits are needed to store a modern IP address.

These numbers are stored by a service called the Domain Name System (DNS). DNS is an automated directory of all of the Internet servers in the world. You can use DNS to look up any server's name and find its IP address.

URL

URL stands for "uniform resource locator".

Every web browser has an address bar at the top of the screen. You enter the URL of a web page into this space. Then the browser will connect to the web server that hosts that page.

The URL is made up of these components, always in this order.

1. The name of the protocol that the page uses. It usually starts with http or https.
2. The domain name. This identifies the server (Internet computer) and website. You could use the web server's IP address here, but that would be more difficult to remember than a name. Also, when a web server hosts more than one website, it would not be able to tell which site you want.
3. The "path name". This identifies a web page on that server.
4. Sometimes extra details are added at the end.

Domain name

The domain name identifies the server that hosts the website. It also identifies the website itself, in case the server hosts more than one. A domain name typically begins with www. It ends with a short text code. This is the "top-level domain". It tells you the general category of the website.

The top-level domain code might tell you the type of business as follows:

- .com – a commercial organisation
- .gov – a US government organisation
- .edu – a US academic organisation such as a university.

Or it might tell you the country where the server is based. Here are some examples:

- .uk – United Kingdom
- .nz – New Zealand
- .ke – Kenya.

The official list of all top-level domains is maintained by the Internet Assigned Numbers Authority (IANA). There are over a thousand top-level domains.

Example

Here is a typical URL. It is for the website of the UK newspaper, *The Guardian*:

http://www.theguardian.com/world. The URL consists of these parts:

- The protocol is "http".
- The top-level domain is ".com". This tells you it is the domain name of a commercial organisation.
- The domain is "www.theguardian.com". This identifies the web server of *The Guardian* newspaper.
- The path name is "/world". This identifies the particular web page of *The Guardian* that summarises world news.

MAC address

MAC stands for "media access control". A MAC address is an identifying number, like an IP address. It identifies a single device such as a computer or printer. A device's IP address is used to route data across the Internet to its local area network, then its MAC address is used to switch the data across the local area network to the device itself. MAC addresses are often shown in hexadecimal form.

Q

Test yourself

1. Why do people prefer to use a URL rather than an IP address?
2. An IP address is 128 bits. How many bytes is that?
3. An IP address identifies every domain on the Internet. What extra information is provided by the MAC address?
4. Here is a URL. Identify the protocol, the domain name and the page:
   https://www.amazon.com/gift-cards

Syllabus reference

1.2.2 Security aspects

Learners should be able to show understanding of the security aspects of using the Internet and understand what methods are available to help minimise the risks.

See also:

Chapter 6 Security

2.3 Safety online

Staying safe

Introduction

The Internet is a wonderful resource. We use it for work, for learning, and to make friendships. However, using the Internet has risks. In this section you will learn how to protect yourself online.

Passwords

Many websites store content that is personal to you, for example payment details or a personal profile. Nobody else should be able to access that content. Websites will protect your personal details with a password. By typing the password you confirm who you are. Unless you type the right password you cannot access the content that is personal to you.

You often have to choose a password when you are working online. Here are some rules about choosing a good password:

- Do not use obvious passwords such as “1234” or “password”. Think of a password that is hard to guess.
- Make sure you can remember the password.
- Do not use the same password on every website.
- Never tell anyone else your password.

Real-life details

Most people using the Internet are friendly. However, there are people using the Internet with bad intentions. Young people are particularly at risk. Never give out your real-life details online. Do not give your full name, address, telephone number, etc. Do not arrange to meet a stranger.

Being careful online

The things you type when you are using the Internet could be stored forever. Your family and friends might see what you wrote. When have a job, your employer might see it. The police and other authorities can see it. It is important not to say cruel, offensive or criminal things. Never type words online that you would not want family, police and employers to see. Never share pictures that you might regret sharing.

Dealing with bullies

Some people make cruel and bullying comments for fun. Perhaps they don't stop and think. Perhaps they just don't care. They can make you feel very upset. It is normal to be upset. Bullying is not caused by anything you did. The bullies are the ones who are wrong.

The best way to deal with online bullying is to block the bully from contacting you. Do not read what the bully writes. You can tell a teacher or other responsible person.

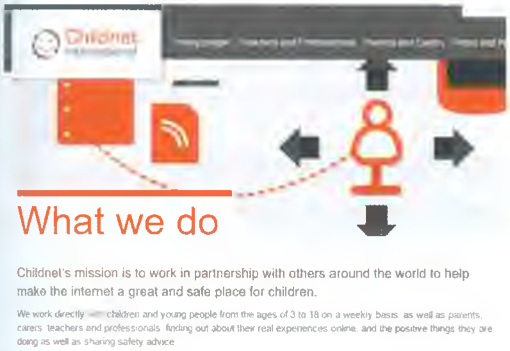
Watch out for tricks

People try to steal money and personal details using online tricks. They set up fake websites. They send emails that pretend, for example, you have won the lottery. Someone might pretend to be a young woman online when he is really an old man. A good rule is to think twice. Only use websites you know. Do not believe every email you receive. Do not open files that a stranger sends you. If you are not sure, ask your teacher for advice.

Advice about staying safe online

There are many good websites offering detailed advice to young people about how to stay safe online. These are available in English and in other languages. Many are operated by charities or governments.

To find websites of this kind, type "staying safe online" into a search engine such as Google. Follow the links to read helpful advice.



What we do

Childnet's mission is to work in partnership with others around the world to help make the internet a great and safe place for children.

We work directly with children and young people from the ages of 3 to 18 on a weekly basis, as well as parents, carers, teachers and professionals, finding out about their real experiences online, and the positive things they are doing as well as sharing safety advice

⬆ www.childnet.com is an international website that gives advice about how to stay safe online

Protective software

You can install software on your computer that protects it against online risks. Learn more about protective software on pages 58–59.

Test yourself

1. Why are you advised not to use the same password on every website?

2. Why is "1234" a poor choice for a password?

3. A schoolboy said "I am going to rob a bank" in an online comment. Why was this a bad idea?

4. A stranger sends you an email asking to meet you. What should you do?

Learning activity

Create a poster for your computer room to remind students how to keep safe online.

Syllabus reference

1.2.2 Security aspects

1.2.3 Internet principles of operation

Learners should be able to show understanding of the Internet risks associated with malware, including viruses, spyware and hacking.

1.5 Ethical issues

Learners should be able to show understanding of ethical issues including hacking.

See also:

6.1 Security threats

Malware and hacking

Introduction

You have learned that there are risks when you use the Internet. Some risks are caused by software that can harm your computer. The general word for this is "malware". Malware is short for "malicious software". It is software made on purpose to harm your computer. In this section you will learn about malware.

Computer viruses

The most common type of malware is a computer virus. A virus is not a complete computer file, it is a set of computer commands. It attaches to a file that is already on your computer. Now the file has extra computer commands, which you didn't intend to be there. The virus copies itself into other files. If any of these is passed to another computer, that computer's files can end up with the virus too. The virus commands are attached to an existing file, so the virus is hidden and you may not know it is there.

Most computer viruses cause significant problems. A virus can:

- delete files or wipe the entire storage
- alter your computer settings
- make your computer carry out actions (such as sending emails).

How does a virus get onto your computer? It might be hidden in a file you download from the Internet. It might be hidden in a file attached to an email. It might be on a storage drive. You should always be careful when you open a file from an unknown source.

Why do people make viruses?

Some people make a virus as a joke or prank. Some people make a virus to make a political protest, to cause trouble, or to harm their enemies. Others make a virus to steal money. Once a virus is made it can spread right around the world. Copies can be passed along Internet connections.

Spyware

Spyware is a special kind of malware. Like a virus, spyware cannot be seen on your computer. Spyware records everything you do with your computer. The person who made the spyware can look at the record of your computer use. That might tell them every website you looked at, and what you typed on your computer.

Spyware can be used by companies and governments to monitor people's behaviour. Spyware is used by criminals to find out your password and personal details.

Types of malware

Often people use the word "virus" to mean any type of malware. In fact, there are many types of malware that are not viruses.

All malware needs to stay hidden from view. Otherwise people would just take it off their computers. The different types of malware use different ways to stay hidden, as follows:

- Virus: this is malware that hides itself inside another file.
- Worm: this is malware in its own file, which copies itself to other computers across the network.
- Trojan: this is malware disguised as a good file, such as a computer game or an image.
- Rootkit: this is malware that changes your operating system (see *5.1 Systems software*) so you cannot spot it.
- Backdoor: this is malware that switches off security software to let other malware onto your computer.

Hacking

You have seen that there are data links between computers. Some people use these data links without permission. They might look at the data on another computer. They might make changes to the data on a computer. This is called hacking.

For example, a hacker might change the data on a bank computer. The hacker might increase the money in his or her account. This is a form of stealing. A hacker might look at government secrets.

Hacking is against the law in most countries. You can go to jail for hacking.

Q

Test yourself

1. What makes a virus different from other types of malware?
2. A student got an email from a person the student did not know. It had a file attachment. Explain why the student should not open the file.
3. A hacker used spyware to find out someone's secret password. Explain what that means.
4. Identify three possible effects of malware.

Q

Learning activity

Write an article for a school magazine, explaining what malware is. Describe the different types of malware.

Syllabus reference

1.2.2 Security aspects

Learners should be able to explain how anti-virus and other protection software helps to protect the user from security risks.

See also:

6.2 Security protection

Protective software

Introduction

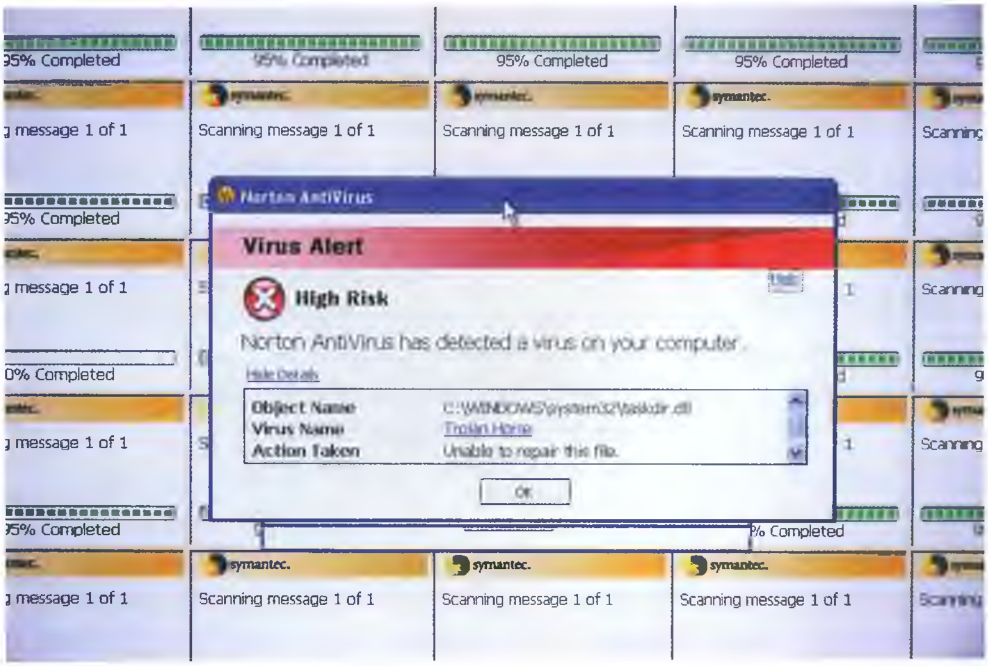
You have learned about malware and other Internet risks. Sensible actions can help prevent those risks. There is software that will help protect you. In this section you will learn about protective software.

Anti-virus software

Remember that malware is hidden. It cannot be seen and removed with ordinary computer usage. Anti-virus software is made specially to stop malware. Anti-virus software will:

- check all new files and emails for malware
- scan your computer to find hidden malware
- delete malware from your computer
- warn you about possible dangers, such as risky websites.

New viruses are being made all the time. Each new virus has special tricks to avoid anti-virus software. Anti-virus software must be updated regularly to keep up with these changes. The update will tell the software about the new viruses that have been invented. Then it can find and delete them all.



Virus Alert

High Risk

Norton AntiVirus has detected a virus on your computer.

Hide Details

Object Name C:\WINDOWS\system32\taskdir.dll
Virus Name Trojan Horse
Action Taken Unable to repair this file.

Symantec is a company that sells anti-virus and other protective software

Spam

Anti-virus software will detect and remove malware. It also has helpful features to protect your computer system from problems other than malware. For example, anti-virus filters will block spam emails.

Spam is a general term for bulk unwanted email. It is sent using automated email systems. A company might send a million spam emails in one go. Spam may contain adverts or fake offers. Often spam emails try to trick you into giving out personal details.

Internet filtering

An Internet filter blocks unsuitable content. An Internet filter is sometimes called a net nanny or parental control software. A filter like this is often set up by parents in a home computer system. The person in charge of the computer system can decide what to block, perhaps based on family rules. An Internet filter could block sites that are unsuitable for children. It could stop users from spending money on the Internet.

Schools and colleges often limit the sites that students can access. Businesses may have similar rules for their employees. This is generally to make sure people use the computer for work purposes, not for social networking or playing games.

Firewall

A firewall is software designed to screen all data that comes from the Internet. The firewall traps every packet of data. It checks the data using programmed rules. It will only pass on data that keeps to the rules. A firewall can prevent many Internet dangers:

- It will stop malware.
- It can prevent hackers getting onto the computer system.
- It can block unsuitable content.

Almost every Internet connection uses some kind of firewall. Business connections may concentrate on preventing access by hackers. Home connections may concentrate on filtering unsuitable content.

Q

Test yourself

1. Why would you use anti-virus software instead of just deleting a virus yourself?
2. My anti-virus software scanned my computer. Why did it do that?
3. I bought anti-virus software two years ago. Why do I need to update it?
4. Why is a firewall a useful feature of a business network?

Q

Learning activities

1. Write a letter to a business owner explaining why he or she should buy firewall software.
2. As a group or a class, find time to talk with the person in charge of the computer system in your school or college. Ask the person about virus protection and any other software that is installed to protect you against risks.
3. What rules should there be about use of the Internet in your school or college? Write a class list titled "Internet policy".

Review

Key terms

Download	When you download web content, you copy it from a web server onto your own computer.
Duplex	A two-way communication link. The signal can go both ways. Both participants act as sender and receiver.
Encryption	A method of protecting data by using a secret coding system.
Internet	The huge network of computer connections that covers the whole world. It uses a set of common protocols so all the connected computers can share data with each other.
Malware	Software designed to harm any computer on which it is held. Malware is usually disguised so you cannot see it on your system or easily remove it.
Parallel transmission	The eight bits which make up a byte of data are sent at the same time along eight different wires.
Peripherals	Hardware devices such as screen, keyboard and mouse that are attached to the processor of a computer.
Protocol	Protocols are communication standards. If two computers share data, they must use the same protocols.
Serial transmission	The eight bits which make up a byte travel along the same transmission medium, one after the other, in a series.
Simplex	A one-way communication link. The signal can only go in one direction from the sender to the receiver.
Transcription error	An error made in copying data, for example when typing it in.
Transposition error	An error where two letters or numbers are in the wrong order.
Upload	When you upload web content, you copy it from your computer onto a web server. That means other computers can access it.
World Wide Web	The collection of all the web pages in the world. Also called "The Web". It is not the same as the Internet.

Project work

One of the extension activities in this chapter was to create a simple web site. If you have not yet done so, find out about a web service which offers free web hosting. As an alternative find out how to create web pages which are hosted by your school's computer system.

As a class, select and upload a range of materials reflecting the work you have done on this course. This can include digital, audio and video materials, as well as items you have found online.

To conclude the project, write a short report on the experience of making a web site or web page. Discuss the software you used and how you decided what items to put on the site.

2 Communication and internet technologies

1 Name the type and method of data transmission being described below:

a Data transmitted in one direction only; one bit at a time over a single channel or wire. [*2 marks*]

....

b Several bits of data transmitted in both directions at the same time over several channels or wires. [*2 marks*]

....

c Data transmitted in both directions, but not at the same time, along a single channel or wire. [*2 marks*]

....

2 a Describe how it is possible to ensure data arrives correctly identified at its destination when using asynchronous data transmission. [*2 marks*]

....

....

....

....

b Describe how it is possible to ensure that data is received in the correct groups when using synchronous data transmission. [*3 marks*]

....

....

....

....

c Give **one** advantage and **one** disadvantage of using synchronous data transmission. [*2 marks*]

Advantage: ....

Disadvantage: ....

3 a Give the meaning of the term **USB**. [*1 mark*]

....

....

b Indicate with a tick (✓) which of the following statements about USB connections are **true**: [*5 marks*]

Statement about USB connections	True (✓)
All the wires in a USB connector are used in data transmission	
The maximum cable length in a USB connection is 2 metres	
Devices plugged into the computer using the USB connection are automatically detected	
The USB connection has become the industry standard for most computers	
The user will always be prompted to download a device driver when the device is plugged in to the computer	

c Give **two** examples of devices which can be connected to a computer using a USB connection. [*2 marks*]

1 ....

2 ....

4 a A system uses **even parity**. Indicate which of the following bytes has even parity: [*3 marks*]

i

1	1	0	0	0	0	1	1

....

ii

1	0	1	1	0	1	1	0

....

iii

0	0	0	1	1	1	1	1

....

b Explain why parity checks are used. [*1 mark*]

....

....

c Nine bytes of data were transmitted from one computer to another computer. **Even parity** was used by both systems. An additional byte, called the parity byte was also sent at the end of the transmission.

The following table shows the nine bytes and parity byte following transmission:

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

i One of the bits has been transmitted incorrectly. Indicate which bit is incorrect by giving its bit number and byte number: *[2 marks]*

bit number: ....

byte number: ....

ii Explain how you arrived at your answer to part **ci**. *[3 marks]*

....

....

....

....

....

....

iii Write down the corrected byte: *[1 mark]*

....

iv Describe a situation where a parity check would not identify which bit had been transmitted incorrectly. *[2 marks]*

....

....

....

....

v Name and briefly describe another method to check if data has been transmitted correctly. *[2 marks]*

....

....

....

....

5 Which internet terms are being described below? *[5 marks]*

Companies that provide the user with access to the internet; a monthly fee is usually charged for this service	
A unique address that identifies the location of a device which is connected to the internet	
A unique address that identifies the device that is connected to the internet	
A set of rules that must be obeyed when transferring files across the internet	
Software that allows a user to display a web page on their computer screen; they translate the HTML from the website	

6 a HTML is made up of **structure** and **presentation**. Explain the difference between these two terms. *[3 marks]*

Structure: ....

....

....

....

....

Presentation: ....

....

....

....

b Indicate how you would know whether or not a website was secure. *[1 mark]*

....

....