6 ICT applications

In this chapter you will learn about:

- communication applications
- data handling applications
- measurement applications
- microprocessors in control applications
- modelling applications
- manufacturing applications
- school management systems
- booking systems
- banking applications
- expert systems
- computers in medicine
- computers in libraries
- computers in the retail industry
- recognition systems
- monitoring and tracking systems
- satellite systems.

This chapter covers a number of applications connected with ICT. Many of the applications bring together notes from earlier and later chapters in the book. Exercises are given at the end of the various sections to help the student develop a better understanding of how these applications make use of various ICT technologies.

6.1 Communication applications

There are several communications systems that make use of ICT technology. For example:

- flyers, posters, brochures and newsletters
- websites
- multimedia presentations
- music scores
- cartoons
- mobile phones
- VoIP (Voice over Internet Protocol)
- business cards and letterheads.

6.1.1 Flyers, posters, brochures and newsletters

Flyers and posters can be produced very easily using one of the many software packages available; most commonly **word processing** and **desktop publishing** software. Usually, the flyer or poster will have photos which have been taken specially or have been downloaded from the internet. The following sequence is fairly typical of how such a document could be produced on a computer system:

1. open a word processor, DTP or presentation application
2. create frames, boxes and/or text boxes
3. take photos if necessary using a camera
4. upload the images from the camera or from a CD/ DVD, scan photos, or download photos from the internet
5. save the photos to a file
6. import or copy and paste the photos into the document
7. edit the photos and import from a file or type any text required.

Brochures can also be used to advertise a company. Whilst these can also be produced on a standard computer and then printed out on a laser or inkjet printer, it is usually more professional to go to a specialist company. These companies will have the ability to print on glossy paper and have access to specialist software producing a better final product.

Brochures and flyers can be sent out to every household in a given area; this will ensure that a certain target group receives a company's advertising. A more 'hit and miss' method is to put the documents inside magazines and newspapers. The big disadvantage of both methods is the tendency to throw the documents away (especially those found in magazines and newspapers) unless they actually catch the eye and offer something interesting or useful.

Whilst we have treated brochures and flyers separately, the actual definition of a brochure can include a flyer, a pamphlet or a leaflet.

Brochures can therefore be a single sheet of paper (folded into two, three or more equal parts) or multiple sheets (either stapled or bound in some other way). Generally, single sheet documents are referred to as flyers or leaflets and booklets are referred to as brochures. Posters tend to be much larger sheets of paper which are displayed on buildings, noticeboards or advertising hoardings.

Posters have the big advantage that they are eye-catching and usually very difficult to miss. They are used in many countries on the sides of roads so motorists see the posters on their way to work. By placing the posters in strategic positions, it is of course possible to target certain people rather than the general public (e.g. advertising expensive cars by placing the posters on buildings or advertising hoardings in financial districts in big cities). The disadvantage is the cost of display (the advertising areas can only be rented) and also they are subject to weather conditions, so only have a limited life.

Newsletters are often produced by companies or clubs using many of the methods described above. They contain local information which is read by company employees or club members. The content is pertinent to the organisation and might include:

- marriages, deaths and births of employees, club members or their families
- fundraising successes by employees or club members
- advertising by outside companies
- news events, such as fundraising, etc.

Figure 6.1 Brochures

Figure 6.2 Flyer/leaflet

Figure 6.3 Poster

6.1.2 Websites

Rather than producing flyers and posters by printing them out, it is possible to use websites to do the advertising. This method of advertising requires the company to either develop their own websites or to pay another company to advertise on their website.

Using the first option requires the company to either employ a team of web designers or go to a specialist company with experience in website design. It will also be necessary to buy hardware and software to develop and store the website. This method can therefore be expensive, but the cost doesn't stop there. It will be necessary to use programmers to make sure that the website is safe from hackers and from pharming attacks. The big advantage is that websites offer world-wide advertising capability and there is also no need to buy paper and other consumables or pay people to deliver leaflets or flyers. Companies have to weigh up the advantages and disadvantages of both methods before they decide which is the best advertising method.

Advantages

- Sound/video/animation can be added.
- Links to other websites/**hyperlinks** can be used.
- Use of **hotspots**.
- Buttons to navigate/move around the website leading to more information.
- Hit counters to see how many people have visited the website.
- Can be seen by a global audience.
- Can't be defaced or thrown away.
- It is much easier to update a website (and there is no need to do a reprint and then distribute the new version).

Disadvantages

- Websites can be hacked into and modified or viruses introduced.
- Risk of potential pharming.
- It is necessary for the potential customers to have a computer and internet connection.
- It isn't as portable as a paper-based system (although with modern smartphones and phablets this is fast becoming untrue).
- Possible for customers to go to undesirable websites (either by accident or as a result of the pharming attack) – this can lead to distrust from customers.
- There is a need for the company to maintain the website once it is set up – this can be expensive.
- Because it is a global system, it is more difficult to target the correct audience using website advertising.

6.1.3 Multimedia presentations

Presentations that use animation, video and sound or music are generally much more interesting than a standard presentation done on slides or paper.

The presentations are produced using one of the many software packages on the market and then used with a **multimedia projector** so that the whole audience is able to see the presentation.

Advantages

- Use of sound and animation/video effects which are more likely to grab the attention of the audience, and can also make the presentation easier to understand.
- It is possible to have interactive/hyperlinks built into the presentation; this means the presentation could access a company's website or even key files stored on the cloud (such as video footage, images, spreadsheets and so on).
- Use of transition effects allow a presentation to display facts in a key or chronological order.
- The presentations can be interactive.
- They are more flexible; because of the links to websites and other external systems (e.g. the cloud), the presentation can be tailored to suit a particular audience.

Disadvantages

- There is a need to have special equipment which can be expensive.
- Equipment failure can be a disaster when giving multimedia presentations.
- Wherever the presentation is given there may need to be internet access.

- There is a danger when using multimedia in presentations that the focus is on the medium (i.e. the multimedia presentation) rather than the message/facts.
- It is very easy to make a bad presentation with too many animation effects and too much text or images.

Paper-based presentations

It is always possible to produce presentations in a hardcopy format rather than the system described above. This has the following advantages:

- disabled people don't have to go to the venue to see the presentation
- it is possible to print it out in Braille for the benefit of blind people
- the recipient can read the presentation at any time they want
- the recipients have a permanent copy which they can refer to at any time they want.

There are, however, disadvantages:

- the presentation needs to be distributed in some way
- there are no special effects (sound, video, animation)
- there are printing costs (paper, ink, etc.).

6.1.4 Music scores

The generation of music and the production of music scores can now be done by computer systems with the appropriate software. Some of the features of this technology include:

- music samplers and mixers allow the original tracks that were recorded in the studio to be modified in any way that the producer wants
- electronic instruments (like guitars and organs) can play back through electronic effects machines
- synthesisers combine simple wave forms to produce complex music creations
- electronic organs can mimic any other instrument
- the music score can be generated from the music itself using software
- software can automatically correct music notes in a score
- there is no real need to understand music notation to write a music score
- music notes are automatically printed out in the correct format.

6.1.5 Cartoons

Animation can be produced using computer hardware and software. With **3-D animation**, objects are designed on a computer and a 3-D skeleton (framework or basic structure) produced. The parts of the skeleton are moved by the animator using key frames (these frames define the start point and end point to give a smooth animation effect). The difference in the appearance of the skeleton in these key frames is automatically calculated by the software and is known as **tweening** or **morphing**. The final stage is to make a realistic image by a technique known as **rendering**.

However, cartoons can simply be freehand drawings and then scanned in or can be computer-generated (possibly with the aid of a graphics pad). The cartoons described in the earlier paragraph are essentially moving images. The example overleaf is a static image but can have the same effect. Essentially, cartoons can add humour to any form of communication and can be a very efficient and effective way to get a message across.

For example:

As with any form of communication, it is important not to offend anybody and also to make sure the cartoon doesn't become the 'main feature' and the message becomes lost somewhere within the humour.

6.1.6 Mobile phones

Note: refer to Chapter 1 for more information on the use of mobile phones.

Mobile phones communicate by using towers inside many cells networked together to cover large areas. The towers allow the transmission of data throughout the mobile phone network.

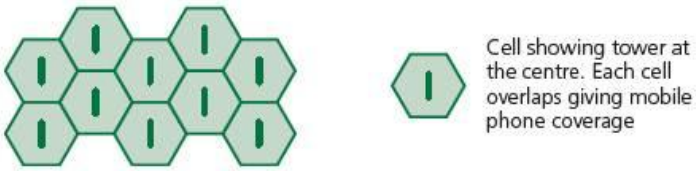


Figure 6.4 Each cell overlaps giving mobile phone coverage

Each tower transmits within its own cell; if you are driving a car and get to the edge of a cell the mobile phone signal starts to weaken; this is recognised by the network and the mobile phone then picks up the signal in one of the adjacent cells. If a person is making a call or sending a text to somebody in a different country then satellite technology is used to enable the communication to take place.

Mobile phone technology can now be used by computers and tablets. A plug-in device (using one of the available USB ports) or **SIM (Subscriber Identity Module)** card allows the computer to connect to the mobile phone network. This then allows access to the internet.

As a communication device, the mobile phone has many advantages.

As the name suggests, they can be used to make phone calls from any location within the cellular network; this has advantages over the more conventional landline system:

- there is no need to look for an operational public telephone in an emergency
- it is possible to conduct business or personal phone calls on the move
- it is easier to keep in contact with co-workers at the office no matter where you are.

They allow text messaging:

- this is quicker and less expensive than making phone calls
- also text messages can be sent at any time of the day even if the recipient's phone is switched off
- they employ predictive texting where the system completes a word from the first few letters keyed in e.g. key in 'preci' and the phone completes the word as 'precious'; predictive texting also allows the system to remember frequently used words – together they increase typing speed.

Mobile phones allow access to the internet on the move using either the cellular network or a Wi-Fi 'hot spot'.

6.1.7 Internet telephony

One of the most common forms of internet telephony (i.e. having a telephone conversation via the internet) is **Voice over internet Protocol (VoIP)**.

Voice over internet protocol (VoIP) is a method used to talk to people using the internet. VoIP converts sound (picked up by the computer microphone or special VoIP telephone plugged into the USB port of the computer) into discrete digital packets which can be sent to their destination via the internet. One of the big advantages is that it is either free (if the talking is done computer to computer i.e. both computers have VoIP telephones or use their built in/plugged in microphones and speakers) or at a local rate to anywhere in the world (when VoIP is used to communicate with a mobile or land line telephone rather than another computer). Obviously, to work in real time this system requires a broadband ISP. The main problems are usually sound quality (echo and 'weird sounds' are both common faults). Security is also a main concern with VoIP, as it is with other internet technologies.

One of the big advantages of using VoIP is that a webcam can also be used so that it becomes a type of video chat. Whilst this doesn't have the sophistication of a video conference, it is much cheaper (no need for special software and additional hardware items – VoIP uses built-in microphones, speakers and webcams). Usually the video quality is not very good, but this can be improved by using a more expensive webcam connected to one of the computer's USB ports.

6.1.8 Business cards and letterheads

Many IT companies offer to produce business cards and letterheads to any design. The user connects to an appropriate website and they will be given a number of business card templates. The user chooses a template and keys in data such as:

- name of company
- contact details
- image wanted on the business card.

The final version of the business card is then shown. The customer places their order and the business cards are printed and delivered.

Business cards can then be handed out to people as a form of personal advertisement. The use of IT (in this case, a website) has made this a much easier task. Business cards are less likely to be thrown away since they are seen as personal contact. It is also possible to include additional information on the reverse of the card – this could be further advertising of the company's products or it could be advertising another company.

Many of the advantages of having business cards are similar to the advantages of using headed stationery.

The same format used on the business cards can be adopted on a company letterhead (as shown on the right). This helps to project a corporate image. As with the business cards, these pages can be printed on high-quality paper using a laser printer.

Flyers and brochures can be produced (as described earlier) using the same design/logo so it becomes very clear to the customer that the communication all comes from one company.

There are several advantages to a company in using corporate letterheads produced by a printing website:

- professionalism (gives a degree of credibility to the company)
- brand/company awareness (advertises the company by using the same designs on all products)
- legal reasons (it helps if there are any legal actions taken – legitimate documents using the company letterhead is regarded as proof of actual communication)
- advertising (the letterhead can contain many useful pieces of information to advertise the company)
- helps to make the company stand out (will tend to have more impact than a white sheets of paper with a typed company heading)
- can make the company appear larger than it is (this could give a degree of confidence to potential customers).

Exercise 6a

Consider the methods of communication covered in Section 6.1 of this chapter.

1 Write an essay on the relative advantages and disadvantages of using websites, multmedia presentations, flyers and brochures to advertise a company's products.
2 Compare technologies such as VoIP and mobile phones as methods of communication. Consider other information found from within the book when discussing your methods.

6.2 Data handling applications

A number of applications make use of simple data handling techniques, such as:

- surveys
- address lists
- clubs and society records
- school reports
- school libraries.

6.2.1 Surveys

Suppose a small business is interested in finding out information about the buying habits of a number of customers. Questionnaires/surveys will be either handed out to people or will be posted on a website to allow them to be filled in online. Paper questionnaires will be filled in either by ticking/shading in boxes, by connecting two points or by filling in ellipses/circles to select the correct response:

A ☐ B ☐ C ☐ D ☐ E ☑ OR A • • B • • C • • D • • E •—•

OR A ⬭ B ⬭ C ⬬ D ⬭ E ⬭

Online questionnaires would tend to use the first option (i.e. using **radio buttons**) since this is a quick and easy method for gathering data.

However, paper surveys have to be scanned in using **OMR** or **OCR** methods and the information is transferred to a database. The advantages of doing this rather than checking each one by hand are:

- faster to get results
- fewer errors
- easier to do a statistical analysis and less expensive (need fewer people).

Online questionnaires have the added advantage that no data preparation is needed at all; the results would be sent directly to a database for analysis.

6.2.2 Address lists

Computers, tablets and mobile phones are all used to store information such as people's home addresses, phone numbers, email addresses or personal data such as date of birth. A typical address book entry may look like the diagram on the right.

The majority of address book applications have features that help the user organise their records into various groupings; such as:

- family
- friends
- work colleagues.

The user can then search by name, grouping, address and so on. Many address book applications also allow synchronisation with tablets and mobile phones. So it is possible to change the data on one system but ensure all devices are kept up to date. As soon as the computer is linked to a tablet or mobile phone then both linked devices will be updated with the latest information.

6.2.3 Clubs and society records

Clubs and societies often keep records of their membership which would typically include: membership number, name, payment details, personal details (phone number, address), their interests etc. A simple database could easily hold all this information making it unnecessary to keep paper records. Consequently, if a particular item of interest (e.g. a talk on F1 motor racing) came up then the computer system could quickly scan all the records on file and find out who would be interested in this topic. They could then automatically contact the member by email or, using mail merge, send out a letter and flyer.

It would also be easy to check on membership subscriptions and send out reminders. This all saves having paper records which are time-consuming to search (and in which details are easy to miss), are easy to lose or misfile, and are more expensive (cost of paper plus filing etc.) and it also saves on space in the office area.

Mail merge is used to find the names and addresses of club members so that reminders can be sent out automatically. The names and addresses would most likely be stored on a database (see further information on mail merge in later chapters).

Record keeping

To evaluate the advantages of using a computer system for record keeping, consider a small bookshop. This shop keeps files on the books in stock and on their customer base. This information could be kept in an electronic form in a simple database. This would make it easy to contact customers if a particular book has just been published or to check on their buying habits. If a customer comes into the shop it would also make it easier to search for a particular book (based on title, author or ISBN). All this leads to several advantages to the shop:

- less office space would be required in the shop since no paper records would need to be kept
- it would be quicker and easier to find details of a particular book or find out whether or not it was in stock
- the system would be less expensive since it wouldn't be necessary to employ somebody to do all the filing and searching
- there would be fewer errors since no manual checking of paper files would need to be done.

There are some disadvantages of the system:

- there would be a need to buy a computer and software to run the system
- time and effort would be required initially to transfer all the existing paper files to the database.

6.2.4 School reports

Computers can be used to keep data on the academic performance of all the students in a school. A database would usually be used to do this. The school could then easily track how well the students were performing over the academic year. The database could be used to produce a printed copy of the student's progress in the form of a report.

This would be considerably easier (and quicker) than writing out a report for each student at the end of the term or year.

A typical database for this application might contain the following fields:

Table 1
StudentID [the student's identification number]
StudName [the name of the student]
TutorGroup [which tutor group the student is in]
Term1Grades [the student's grades for the first term]
Term1Attend [the student's attendance record for the first term]
Term1Notes [this may contain teacher notes about the student's performance]

There may be tables for term 2 and term 3 so that the database contains all the data for the students over the full academic year.

The majority of databases allow the teachers to produce professional-looking reports by carrying out a series of queries. Headed notepaper with the school's name (and possibly logo) will also enhance the appearance of the report.

FIRE Academy

Semper sursum
Student: 123456 John Doe
Term: end of July 2015

Subject	Grade
Mathematics	A
Science	B
History	D
Languages	E
Art	C
Music	B

Attendance: 97%

Comments: John has continued to work well. He has done particularly well in Maths, Science and Music. His attendance also continues to be excellent.

Mail merge is used to find the names and addresses of parents so that reports can be sent out automatically. The names and addresses would most likely be stored on a database (see further information on mail merge in later chapters).

6.2.5 School libraries

Please refer to Section 6.12 for more details on this topic.

6.3 Measurement applications

Measurement applications, using sensors and other electronic hardware (such as a microprocessor), are many and varied.

This type of application involves sensors constantly taking measurement data (such as temperature, rate of rotation or light intensity). Because the data from the sensors are often in an analogue form, they have to be sent to an **Analogue to Digital Converter (ADC)** to turn the data into a digital format. This is needed because microprocessors and computers only understand digital data.

Advice

Some textbooks will use the term 'signal' instead of data.

The term '**analogue**' means the data is constantly varying and has no discrete values (e.g. the height of mercury in a thermometer to represent temperature). The term '**digital**' refers to discrete data which is made up from the binary values 0 and 1. When controlling devices such as pumps, valves, heaters, etc., data/signals (a series of 1s and 0s) from the computer often need to be converted back into an analogue form (e.g. electric signals) using a **Digital to Analogue Converter (DAC)**.

After conversion, the data is sent to a microprocessor where it is processed. However, in measurement applications, the microprocessor simply reviews the data from the sensors (by sometimes comparing it to data stored in memory) and updates its files and sometimes gives a warning signal if the values are outside given parameters. *The microprocessor will take no action to change any of the conditions during the measurement process.*

Examples of measurement applications include:

- weather stations
- scientific experiments (e.g. taking temperature measurements)
- measuring a patient's vital signs on a hospital
- pollution monitoring
- burglar alarm systems.

6.3.1 Weather stations

Weather stations are set up to automatically gather data from the environment. They are usually unmanned and use a variety of sensors to measure:

- rainfall
- temperature
- wind speed
- wind direction
- (barometric) pressure (air pressure)
- humidity.

The data needs to be gathered 24/7 (i.e. 24 hours a day, every day). This data can then be used by weather forecasters to help predict the weather for the next few days or take a more long-term view by looking at weather patterns.

6.3.2 Measuring a patient's vital signs in a hospital

The following steps show what happens when a computer is used to measure the key vital signs of a patient in a hospital:

- sensors read key vital signs (such as pulse rate, heart rate, temperature, blood pressure, respiration, etc.)
- the data from the sensors is converted into digital using an ADC
- the data is stored in the computer's memory
- the computer compares the data from the sensors with the values stored in its memory (these will be input by the nurse or doctor for a particular patient)
- the results are output on a screen in the form of graphs and/or numerical readouts
- an alarm is activated if any of the data is outside acceptable input values
- the system continues to measure the patient's vital signs until the computer is turned off.

6.3.3 Measuring pollution in a river

The following steps show what happens when a computer is used to measure pollution in a river:

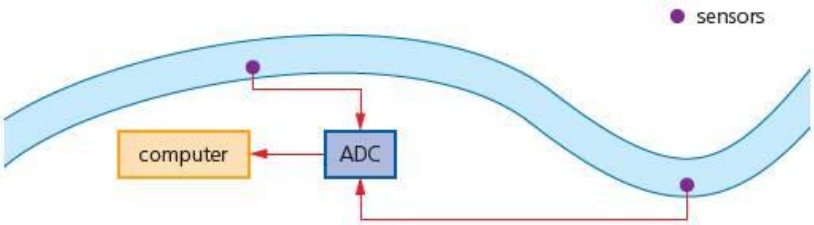


Figure 6.5 Sensors read data from the river (oxygen levels and acidity levels – pH sensor)

- the sensors are placed in at least two different positions so that a pollution comparison can be made
- the data from the sensors is converted into digital using an ADC and sent to a computer
- the computer stores the received data
- the oxygen levels and acidity levels are compared to the historical data stored in memory and they are also compared to *pre-set levels* stored in memory
- the oxygen and acidity levels from the different positions in the river are also compared to see if they are similar – this is used to see if the source of the pollution can be found.

One of two things will now happen: *either* the data is transferred to a CD/DVD or to a memory stick and taken away for further analysis *or* the computer is connected to a mobile phone network and transmits the data back automatically to the monitoring station.

Other sensors, such as light sensors (to see if there are solids or chemicals in the water blocking out light), can also be used.

Advantages

- The computer wouldn't forget to take readings.
- The computer's response time is much faster (very important in the hospital monitoring application).
- Doctors, nurses, scientists, etc. can all get on with other tasks whilst the measurements are taken automatically.

- Computers give 24-hour cover every day.
- The readings will tend to be more accurate.
- Readings can be taken more frequently if done by a computer and sensors.
- It could also be safer since whatever is being measured may have potential hazards (e.g. children falling into the river whilst attempting to take readings or a nurse looking after a patient who has a contagious disease).
- Computers can produce graphs automatically for analysis of results.
- There is a potential cost saving as fewer staff are needed since the measurements are now done by computer (which results in a reduced wages bill).

Disadvantages

- The computer is unable to respond to unusual circumstances.
- Computer equipment and measuring software can be expensive to purchase and set up in the first place.
- A student doing an experiment, for example, will rely on the computer doing the measurement and analysis – it is possible the student will not learn as much using a computer system.
- If the computer malfunctions or if there is a power cut, then the computer cannot be used, and there needs to be good backup procedures in place to cover this eventuality.

Exercise 6b

A student is carrying out an experiment to measure the temperature of a liquid over a 30-minute period. This involves noting down the temperature from a thermometer placed in the liquid; readings are taken every 20 seconds. At the end of the 30 minutes, the student draws a graph of temperature against time:

The teacher in charge of the science lesson has decided to do the experiment using sensors and a microprocessor.

1 Describe how the experiment would now be carried out using sensors and microprocessor.
2 Describe the main advantages of doing the experiment using sensors and a microprocessor.

Exercise 6c

A burglar (intruder) alarm system uses various sensors and a microprocessor to detect the presence of intruders. The alarm is set up by keying in a six-digit PIN on a control panel.

1 Name three suitable sensors for this application.
2 Describe how the sensors and microprocessor interact to warn of the presence of an intruder.

6.4 Microprocessors in control applications

In control applications, sensors and a microprocessor or computer are again used. Sensors send data to the microprocessor or computer which then compares the incoming data to stored values or data entered earlier on. As with measuring applications, an ADC may be needed before the microprocessor/computer can process the data.

The microprocessor/computer will check whether the incoming data is outside the given parameters and will take any necessary action. For example, a temperature sensor sends data to a computer which will then check whether the temperature is greater than the preset or stored value. If the temperature is greater than the preset value, the computer will send a signal to switch off a heater. If the temperature is less than the preset value, the computer will send a signal to switch on a heater. There are, of course, many other examples. Unlike measurement applications, the microprocessor/computer will take some action which will ultimately affect the next input value it receives. By doing this, the microprocessor/computer is controlling the application.

Some control applications include:

- automatic washing machines
- automatic ovens/cookers
- central heating systems
- chemical plants
- glasshouse environment control.

Exercise 6d

Find out how sensors are used in automatic washing machines.

6.4.1 Automatic oven/cooker

An automatic cooker/oven has temperature sensors and a number of controls to set the cooking time (i.e. when to switch the cooker/oven on and off). First of all, the start time and end time (or the actual cooking time) are entered. Finally, the cooking temperature is selected.

The microprocessor checks the set time against the current time and when they are equal, the cooker/oven heating elements are switched on. Once the cooker/oven starts the cooking process, the microprocessor then constantly checks the end time against current time (the end time may be a pre-set value entered by the user or it may be a value calculated by the microprocessor, based on the cooking time entered); when they are equal, the cooking process is stopped.

The microprocessor checks the temperature data sent from a sensor and turns the heating element on if the value less than the preset value chosen by the user. If the temperature is great than or equal to the preset value, then the heating element is switched off by the microprocessor.

Once the cooking process is finished, the microprocessor sends a signal to a beeper to making a beeping sound to indicate that the cooking cycle is completed.

6.4.2 Central heating systems

In the example in Figure 6.6, a gas supply is used to heat water in a boiler. A valve on the gas supply is controlled by a microprocessor and is opened if the heating levels need to be increased. A water pump is used to pump hot water around the central heating system whenever the temperature drops below a preset value.

Note: the water pipes and radiators are not shown in the diagram; only those parts controlled by the microprocessor are shown.

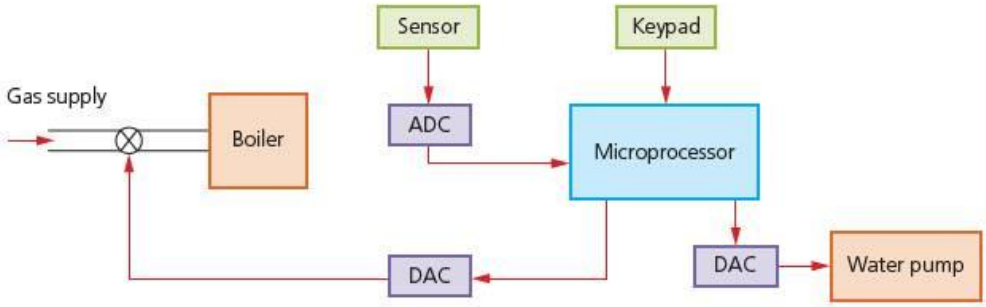


Figure 6.6 A central heating system

So how does this work?

- The required temperature is keyed in and this is stored in the microprocessor memory (this is called the preset value).
- The temperature sensor constantly sends data readings to the microprocessor.
- The sensor data is first sent to an ADC to convert the analogue data into digital data.
- The digital data is sent to the microprocessor.
- The microprocessor compares this data with the preset value.
- If the temperature reading greater than or equal to the preset value then no action is taken.
- If the temperature reading is less than the preset value, then a signal is sent:
  - to an actuator (via a DAC) to open the gas valve to the boiler
  - to an actuator (via a DAC) to turn on the water pump.
- The process continues until the central heating is switched off.

Exercise 6e

Find out how sensors and microprocessors are used to control the following central heating systems:

1. one which uses an oil burner as the source of heat
2. one which uses electric radiators that are switched on and off by the microprocessor.

6.4.3 Chemical process control

A certain chemical process only works if the temperature is above 70°C and the pH (acidity) level is less than 3.5. Sensors are used as part of the control system. A heater is used to heat the reactor and valves are used to add acid when necessary to maintain the acidity. How the sensors and computer are used to control this process is described below:

- temperature and pH sensors read data from the chemical process
- this data is converted to digital using an ADC and is then sent to the computer
- the computer compares the incoming data with preset values stored in memory if the:
  - temperature is less than 70°C, a signal is sent to switch on the heaters
  - temperature is greater than or equal to 70°C, a signal is sent to switch off the heaters
  - pH is greater than 3.5, then a signal is sent to open a valve and acid is added
  - pH is less than or equal to 3.5, then a signal is sent to close this valve
- the computer signals will be changed into analogue signals using a DAC so that it can control the heaters and valves
- this continues as long as the computer system is activated.

6.4.4 Glasshouse environment control

Five different sensors could be used here to control the glasshouse environment; namely, humidity, moisture, temperature, pH and light. To simplify this problem the control mechanisms are shown in Figure 6.7.

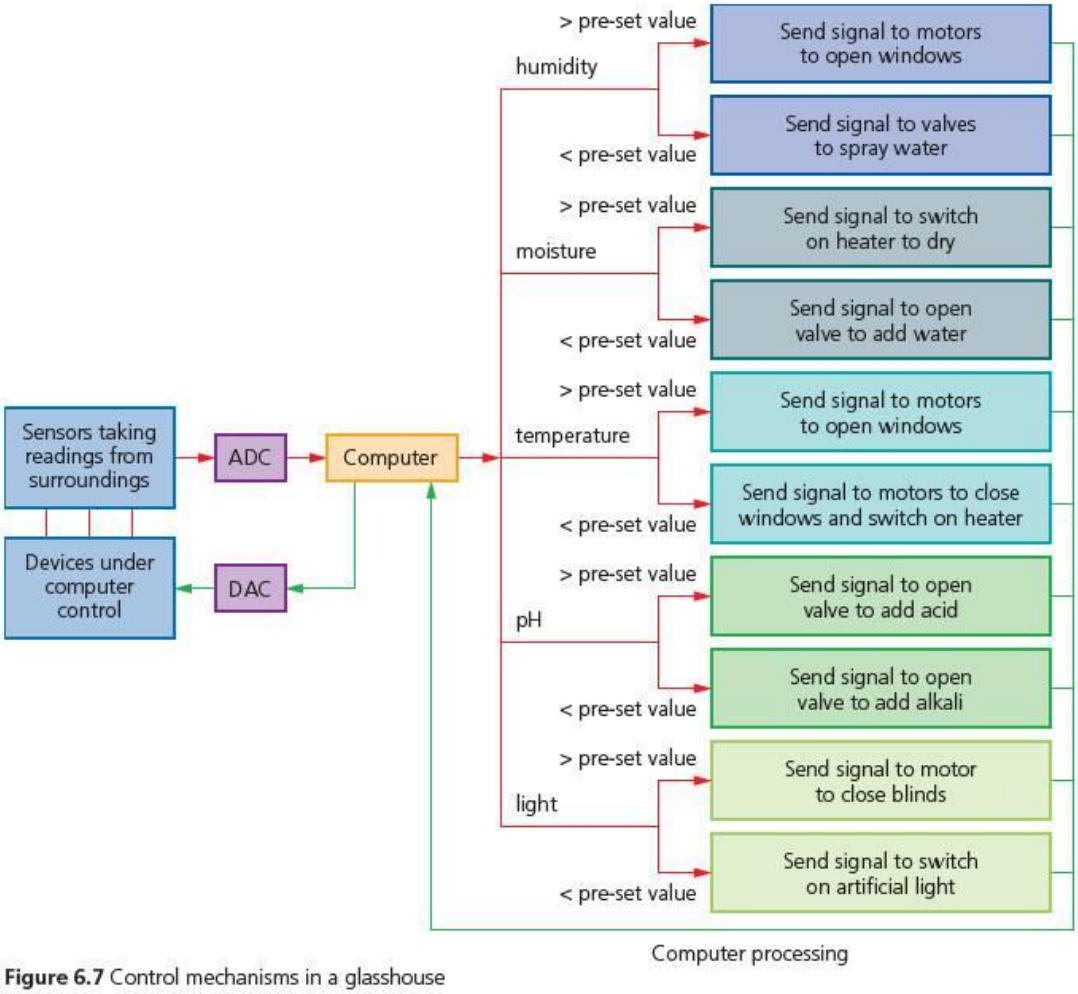


Figure 6.7 Control mechanisms in a glasshouse

Because of the number of sensors, this is clearly quite a complex problem. Let us consider the humidity sensor only. This sends a signal to an ADC which then sends a digital signal to the computer. This compares the input with stored (preset) values and decides what action needs to be taken (follow the orange lines in the diagram above). If humidity is greater than (>) the preset value, the computer sends a signal to a DAC to operate the motors to open windows thus reducing the humidity. If it is less than (<) the preset value, the computer sends a signal to open valves to spray water into the air (follow the green lines in the diagram above). If the reading is the same as the preset value, then no action is taken (this isn't shown in the diagram since it could follow either direction). The control process continues as long as the system is switched on. Similar arguments can be used for all five sensors.

The table on the next page gives a list of possible sensors that might be used in various applications which involve measurement or control.

Sensor type	Possible applications
Temperature	used in the control of central heating systems
	used in the control of/measuring temperatures in a chemical process
Moisture	measuring/used in the control of a glasshouse environment
	measuring moisture levels in any process (e.g. in the production of electronic components)
Oxygen/carbon dioxide	environment monitoring (e.g. measuring the oxygen content in a river to check for pollution)
	measuring carbon dioxide levels in a glasshouse
Light	measuring the light levels in a glasshouse
	measuring for light levels in a dark room (photography)
	used with automatic doors
Infra-red	detecting an intruder by the breaking of an infra-red beam
	allows microprocessor to count items
Pressure	detecting intruders in a burglar alarm system
	counting vehicles as they pass over a bridge
Acoustic	picking up sounds (e.g. footsteps when used in a burglar alarm system)
	detecting liquids or solids moving in pipes/check for blockages in pipes
Motion	detecting movement (as in virtual reality interface devices)
pH	measuring acid/alkaline levels in a river (pollution monitoring)
	used in a glasshouse to measure soil acidity/alkalinity
	used to measure acidity in a chemical process
Proximity/distance	these tend to be another name for the above sensors such as infra-red, motion, etc.)

Exercise 6f

1 i Name the sensors needed in the control of an automatic washing machine.
ii Describe how sensors and a microprocessor are used to control the wash cycle in an automatic washing machine.

2 Look at Figure 6.7 on page 98. Describe how the pH sensor and light sensor are used to control the soil acidity and light levels in the glasshouse.

3 A street lamp is turned on when it is dark and is switched off when it becomes light again. What sensor is needed to determine whether it is dark or light?
Describe how the sensors and microprocessor are used to control the switching on and off of the street lamp. Take into account situations such as very heavy cloud cover so that the lamp isn't switching on and off every 30 seconds.

Why use sensors and computer systems to control processes?

A number of advantages were given earlier under the measurement applications section; these advantages are also valid for control applications. There are a couple of additional advantages to consider:

- the response time, if some parameter is out of range, is much faster
- if a process is dangerous it is better to control it from a distance.

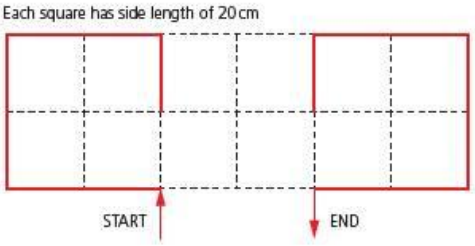
The disadvantages are very similar to those given earlier for measurement applications using computers and microprocessors.

6.4.5 Turtle graphics

This is based on the computer language called LOGO and is now usually known as **turtle graphics**. This is essentially the control of the movement of a 'turtle' on a computer screen by a number of key commands which can be typed in.

The most common commands are:

Command	Meaning
FORWARD **x**	Move **x** cm forward
BACKWARD **x**	Move **x** cm backward
LEFT **d**	Turn left through **d** degrees
RIGHT **d**	Turn right through **d** degrees
REPEAT **n**	Repeat next set of instructions **n** times
ENDREPEAT	Finish the repeat loop
PENUP	Lift the pen up
PENDOWN	Lower the pen



Two different ways to draw this shape are shown below. Option 1 uses a sequence of commands that draw the shape line by line. However, option 2 is a more efficient technique that uses the REPEAT and ENDREPEAT commands. This is used when repeating sequences exist which can be enclosed inside the REPEAT … ENDREPEAT construct. For example:

```
10  RIGHT 50
20  FORWARD 30
30  RIGHT 50
40  FORWARD 30
50  RIGHT 50
60  FORWARD 30
70  RIGHT 50
80  FORWARD 30
90  RIGHT 50
100 FORWARD 30
110 RIGHT 50
120 FORWARD 30
```

This sequence consists of six repeating commands:

```
RIGHT 50
FORWARD 30
```

and we can therefore write the whole sequence as:

```
10  REPEAT 6
20  RIGHT 50
30  FORWARD 30
40  ENDREPEAT
```

which is considerably more efficient since it only needs four lines rather than 12.

Thus, to draw the shape shown earlier we have the two possible solutions shown in the table on the next page (option 2 makes use of the REPEAT … ENDREPEAT construct).

Option 1 instructions		Option 2 instructions	
PENDOWN	FORWARD 40	PENDOWN	PENDOWN
LEFT 90	LEFT 90	LEFT 90	FORWARD 20
FORWARD 40	PENDOWN	REPEAT 3	REPEAT 3
RIGHT 90	FORWARD 20	FORWARD 40	RIGHT 90
FORWARD 40	RIGHT 90	RIGHT 90	FORWARD 40
RIGHT 90	FORWARD 40	ENDREPEAT	ENDREPEAT
FORWARD 40	RIGHT 90	FORWARD 20	
RIGHT 90	FORWARD 40	PENUP	
FORWARD 20	RIGHT 90	LEFT 90	
PENUP	FORWARD 40	FORWARD 40	
LEFT 90		LEFT 90	

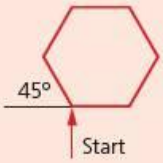
Exercise 6g

Show how the following sequence could be simplified by using the REPEAT … ENDREPEAT construct wherever possible:

10	PENDOWN	100	LEFT 72
20	LEFT 90	110	PENUP
30	FORWARD 80	120	FORWARD 100
40	RIGHT 72	130	PENDOWN
50	FORWARD 80	140	FORWARD 50
60	RIGHT 72	150	RIGHT 90
70	FORWARD 80	160	FORWARD 50
80	RIGHT 72	170	RIGHT 90
90	FORWARD 80	180	FORWARD 50
		190	PENUP

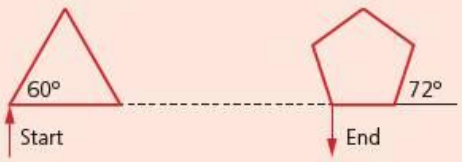
Exercise 6h

1 Use the REPEAT …. ENDREPEAT commands wherever you can to draw the following shape:



Each side is length 30 mm and the angle shown is 45°.

2 Use turtle graphics to draw the following two-shape drawing. Each side of the regular triangle is 50 mm and each side of the regular pentagon is 30 mm. The angles in the triangle are 60° and the angle shown in the pentagon is 72°. (The distance between the two shapes is 120 mm.)



6.5 Modelling applications

A **computer model** is the creation of a **model** of a real system in order to study the behaviour of the system. The model is computer generated and is based on mathematical representations.

The whole idea is to try to find out what mechanisms control how a system behaves. This then makes it possible to predict the behaviour of the system in the future and also see if it is possible to influence this future behaviour.

Computer models have the advantage that they save money, can help find a solution more quickly and can be considerably safer (more of this later). There are many examples of computer models which range from simple spreadsheet representations through to complex flight simulators. The following simple example uses a spreadsheet to do the modelling of a tuck shop in a school:

	A	B	C	D	E	F
1	Item name	Price each ($)	Selling price ($)	Profit per item	Number sold	Total profit per item ($)
2						
3						
4	chew	1.00	1.50	0.50	35	17.50
5	chox	2.00	2.50	0.50	45	22.50
6	gum	3.00	3.50	0.50	30	15.00
7	crisps	1.00	1.50	0.50	45	22.50
8	cake	2.00	2.50	0.50	40	20.00
9						
10					Profit/Loss ($)	-102.50

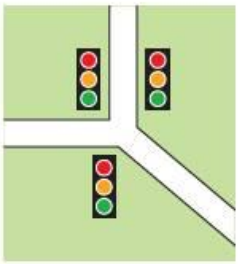
The formulae behind this spreadsheet are:

	A	B	C	D	E	F
1	Item name	Price each ($)	Selling price ($)	Profit per item	Number sold	Total profit per item ($)
2						
3						
4	chew	1.00	1.50	=(C4-B4)	35	=(D4*E4)
5	chox	2.00	2.50	=(C5-B5)	45	=(D5*E5)
6	gum	3.00	3.50	=(C6-B6)	30	=(D6*E6)
7	crisps	1.00	1.50	=(C7-B7)	45	=(D7*E7)
8	cake	2.00	2.50	=(C8-B8)	40	=(D8*E8)
9						
10			Weekly shop cost	200.00	Profit/Loss ($)	=SUM(F4:F8)-D10

Thus by varying the values in column C or in column E it would be possible to model the shop's profit or loss. This is a very simple model but it shows the principal of using spreadsheets to carry out any type of modelling that can be represented in a mathematical form.

Traffic light simulation

A set of traffic lights are to be modelled at a Y-junction:



In this computer model it is necessary to consider:

i How and what data needs to be collected.
ii How the computer model is carried out.
iii How the system would work in real life.

How and what data needs to be collected?

Since the success (or failure) of a computer model depends on how realistic it is, data needs to be collected by watching traffic for a long period of time at the Y-junction. This is best done by using induction loop sensors which count the number of vehicles at each junction. Manual data collection is possible but is prone to errors and is difficult to do over an 18-hour period per day (for example). The sort of data that would need to be collected or considered for collection is as follows:

- a count of the number of vehicles passing the junction in all directions at all different times of the day
- the day of the week (weekends, bank holidays, etc. can alter how the data need be interpreted)
- how long it takes a vehicle to clear the junction

- how long it takes the slowest vehicle to pass through the junction
- whether there are any pedestrian crossings etc. nearby
- whether there are other factors which might affect the junction (e.g. left turns, right turns, filtering, etc.).

How is the computer model carried out?
Data from the above list is entered into the computer and the computer model is run. Once the designers are satisfied that it models the real situation accurately (i.e. by comparing results obtained with actual traffic flow from a number of data sets) then different scenarios can be tried out. For example:

- vary the timing of the lights and see how the traffic flow was affected
- increase the number of vehicles stopped at part of the junction and then change the timing of the lights to see how the traffic flow is affected
- increase or decrease traffic flow in all directions
- consider how emergency vehicles affect traffic flow at different times of the day.

How would the system work in real life?

1. Sensors in the road gather data and count the number of vehicles at the junction.
2. This data is sent to a control box or to a computer (it may need to be converted first into a form understood by the computer).
3. The gathered data is compared to data stored in the system (the stored data is based on model predictions which were used to optimise the traffic flow).
4. The control box or computer 'decides' what action needs to be taken.
5. Signals are sent out to the traffic lights to change their timing if necessary.

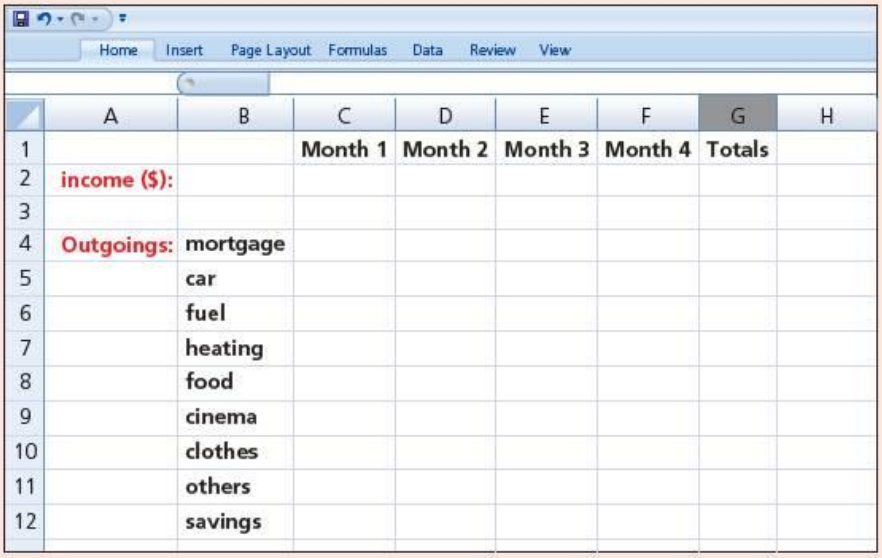
Why are computer models done (in general terms)?

- They are less expensive than having to build the real thing (e.g. a bridge!).
- On many occasions it is safer to run a computer model (some real situations are hazardous e.g. chemical processes).
- With computer models it is much easier to try out various scenarios in advance.
- It is nearly impossible to try out some tasks in real life because of the high risk involved or the remoteness (e.g. outer space, under the sea, nuclear reactors, crash testing cars, etc.).
- Time scales are reduced by doing a computer model rather than the real thing (some applications would take years before a result was known e.g. climate change calculations, population growth, etc.).

Other examples of computer models include: population growth, modelling queues at checkouts, training pilots and drivers, running chemical and nuclear plants, crash testing of cars, financial modelling and weather predictions.

Exercise 6i

Create a spreadsheet to do some personal financial modelling. Include the monthly income in one row and then show all the monthly outgoings. For example:



	A	B	C	D	E	F	G	H
1			Month 1	Month 2	Month 3	Month 4	Totals	
2	income ($):							
3								
4	Outgoings:	mortgage						
5		car						
6		fuel						
7		heating						
8		food						
9		cinema						
10		clothes						
11		others						
12		savings						

Extend the list as much as you want or change the outgoings to be more realistic if necessary. Insert some values into the spreadsheet and then change a few values to see the effect on your finances. Add extra columns or extra outgoings to extend the spreadsheet. Finally try graphing your income against outgoings for each month and for a year (do a prediction for the year after four months, for example).

Exercise 6j

Here is a list of five computer models and also a list of five reasons why models are carried out. Try to match the five models to the best reason why that model would be done.

Model	Reason
PILOT TRAINING	Cost of building the real thing is too expensive
ENVIRONMENTAL MODELLING	Some situations are too dangerous to humans
MODELLING BRIDGE LOADING	Take too long to get results back from real thing
NUCLEAR REACTOR MODEL	It is almost impossible to do the tasks for real
SPACE EXPLORATION	Easier/safer to make changes to a model

6.6 Manufacturing applications

Manufacturing uses ICT (i.e. automation) in a number of areas to improve productivity, reduce costs, improve consistency and to make factories safer and more environmentally friendly.

One of the most common forms of automation is the use of robots.

Robotics

Robots are used in many areas of manufacturing, from heavy work right through to delicate operations. Examples include: paint spraying of car bodies, welding bodywork on cars, manufacturing of microchips, manufacturing electrical goods and automatic warehouses.

Control of robots is either through embedded (built-in) microprocessors or linked to a computer system. Programming of the robot to do a series of tasks is generally done in two ways:

1 The robot is programmed with a sequence of instructions which allow it to carry out the series of tasks (e.g. spraying a car body with paint).
2 Alternatively, a human operator manually carries out the series of tasks; this can be done in two ways. In our example, we will assume an object is being painted using a robot arm.

   i The robot arm is guided by a worker when spraying the object; each movement of the arm is stored as an instruction in the computer.

   OR

   ii The worker straps sensors to his own arm and sprays the object; each movement is stored as a set of instructions in a computer; the sensors send back information such as position relative to the object, arm rotation, and so on – this information forms part of the instructions stored in the computer.

Whichever method is used, once the instructions have been saved, each series of tasks can then be carried out by a robot arm automatically. Each instruction will be carried out identically every time (e.g. assembling parts in a television) giving a consistent product.

Robots are often equipped with sensors so they can gather important information about their surroundings and also preventing them from doing 'stupid things' e.g. stopping a robot spraying a car if no car is present, or stop the spraying operation if the supply of paint has run out, etc.

Robots are very good at repetitive tasks. However, if there are many different tasks (e.g. making specialist glassware for some scientific work) then it is often better to still use human operators.

Figure 6.8 Robot arm equipped with a spray gun 'end effector'. Different end effectors allow the robot arm to carry out many different tasks

Advantages

- They can work in environments harmful to human operators.
- They can work non-stop (24/7).
- They are less expensive in the long term (although expensive to buy initially, they don't need wages).
- Higher productivity (don't need holidays, etc.).
- Greater consistency (e.g. every car coming off a production line is identical).
- They can do boring, repetitive tasks leaving humans free to do other more skilled work (e.g. quality control or design work).

Disadvantages

- They find it difficult to do 'unusual' tasks (e.g. one-off glassware for a chemical company).
- They can cause higher unemployment (replacing skilled labour).
- Since robots do many of the tasks once done by humans, there is a real risk of certain skills (such as welding) being lost.
- Because robots are independent of the skills base, factories can be moved anywhere in the world (again causing unemployment).
- The initial set-up and maintenance of robots can be expensive.

Exercise 6k

Which of these are advantages and disadvantages for the employees and which are for the employers?

6.7 School management systems

Schools have to manage a number of different tasks in the day-to-day running of the school. These include:

- registration and attendance records of the students
- student performance
- organisation of school exams (internal and external)
- creation of timetables
- teacher substitution (when teachers are absent due to illness or training).

6.7.1 School registration systems

The traditional way to record the registration and attendance of a student was to complete daily registers. This was very time consuming since it required a 10-minute session at the beginning and end of each day. It was also prone to error if a student's name was missed at some point during the registration process. There are now a number of possible ways of automating the registration process using hardware and software, some of which are included below.

Method 1

Issue each student with an ID card. This would contain a magnetic stripe (shown in black) on the rear of the card. The student would have to sign the card and also write his unique student ID on the back of the card as well. The magnetic stripe would contain the name of the school, the name of the student, the student's data of birth and their unique ID (registration) number.

Each morning the student would arrive at the school and swipe their ID card through a magnetic card reader. The data read would identify the student and the time and date they entered the school's premises. This data would now be stored on a database. On leaving the school (either at lunchtime or at the end of the day), the ID card would again be swiped. This would now record the leaving time

and date on the database. This would give a very comprehensive record of when the student attended the school and the number of hours they attended. It would also be a more secure method in the event of, for example, a fire. The school would now be able to account for every student currently showing as being present on the school premises. Using the paper-based system, a student could register then just go home – with this ID card system, the student's attendance would be known at all times.

There are further subtleties that could be used such as (1) use of a PIN to stop another student swiping in with the wrong card (2) use of GPS tracking (see Section 6.16.1) so the exact whereabouts of a student would be known; this would require the addition of a chip in the ID card so that the tracking system could identify them (this is the basis of RFID which was discussed in Chapter 2). At the end of a term (or school year), the database could be interrogated and it would give an accurate attendance record for the student.

Method 2

A second method could make use of biometrics. Each student would have their fingerprints taken. Their personal details (as in method 1) plus fingerprints would be stored on a database. When a student entered the school premises, they would be asked to put their hand on a scanner which would read their fingerprints. Since each student would have unique fingerprints, this system would be very secure. As with method 1, the date and time of entering or leaving the school would be accurately recorded on the database.

Advantages

- Fingerprints are unique, so it would be impossible for a student to sign in pretending to be someone else (with magnetic cards, a student could give his card to a friend and ask them to sign in for him) – this gives more accurate data and improved security.
- ID cards could easily be lost – fingerprints are 'part of you' so can't be lost.
- ID cards could be affected by magnetic fields (e.g. by being placed close to a mobile phone) which would stop them working.
- It is much easier to 'clone' (i.e. make copies of) ID cards than it would be to copy fingerprints (not impossible but very difficult).

Disadvantages

- It would take a long time to collect the initial fingerprints for every student in the school.
- The equipment needed to take and read fingerprints is more expensive than magnetic stripe reading equipment.
- If a student cuts a finger, the fingerprint may not be identified by the system (which would prevent entry to the school).
- There are 'invasion of privacy' issues and some parents may object to having the fingerprints of their children stored on a database.

6.7.2 Student performance

Teachers could make considerable use of spreadsheets to monitor the performance of their students. This was discussed in Section 5.1. Essentially, spreadsheets could record the test results of each student over a term/year. This would allow a teacher easily to see how they were performing against other

students in the same subjects. It would also be easy to import data into a report, for example, summarising a student's performance over the academic year.

6.7.3 Exam timetables, subject timetables and teacher substitution

Timetables are often required for the following:

- exams scheduling (both internal and external)
- subject scheduling
- producing cover/substitution plans for teachers who are absent.

For example, at the start of a new academic year, a student may be given their own personal timetable covering their subject allocation:

Timetable for: Paul Smith 012 234 555 Summer term 2016					
	09:00–10:30	10:40–12:10	12:20–13:20	13:30–15:00	15:10–16:40
Monday	Mathematics	History	*lunch*	Science	Science
Tuesday	Geography	Art/Music	*lunch*	ICT	ICT
Wednesday	Sport time	Sport time	*lunch*	Art/Music	Geography
Thursday	Geography	History	*lunch*	Mathematics	Art/Music
Friday	ICT	Mathematics	*lunch*	Science	History

Many factors have to be taken into account when producing timetables for each student:

- availability of teachers
- availability of rooms for each subject
- subject clashes (e.g. a student wishing to do French from a group containing French, History, English and Spanish finds this clashes with their Art/Music lessons and so they have to take History instead of French)
- number of hours for each subject
- making sure double lessons appear for certain practical subjects but ensuring this doesn't happen with others.

Timetables are also produced so that students know when to sit an exam. This allows them to schedule their work correctly.

The main advantages of using software to create timetables is that it is quicker and less error-prone than the older paper-based systems. It is also easier to try 'what if' scenarios to ensure the most efficient use of time is utilised.

Likewise, timetables can be produced to cover classes when teachers are absent. This is often done using the main timetable software since each teacher is allocated a class or non-contact time for each of the teaching periods. In the example above, a teacher would have either a class or a 'free period' for each 1.5 hour session. The main subject speciality of each teacher is also stored so that a subject specialist can be used to cover for absent teachers.

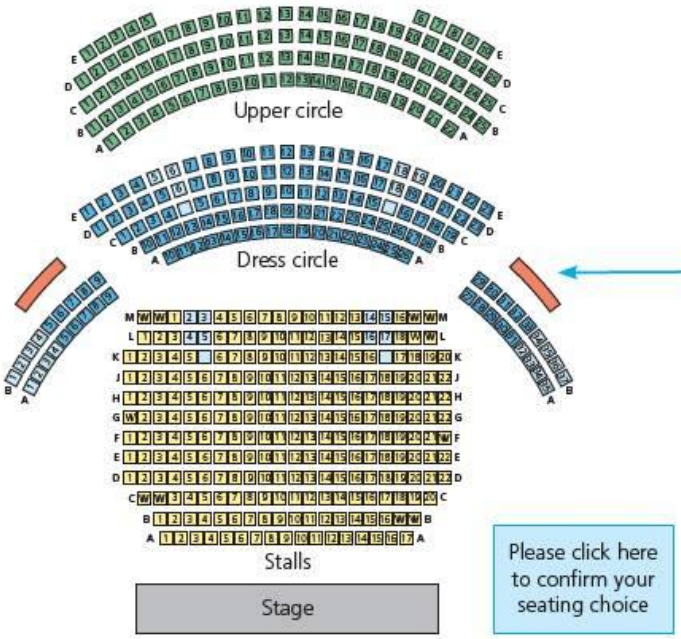
6.8 Booking systems

6.8.1 Theatre and cinema booking systems

Online booking systems rely on the ability to update files immediately thus preventing double-booking etc. which could happen if the system response time was slow. Booking systems are used for transport (flights, trains and buses), cinemas and theatres.

We will consider the theatre booking system to describe how this system works. With this example, we have assumed that the customer has already logged on to the theatre booking website:

- the customer clicks on the performance they wish to see
- a date and time is typed in
- the required number of seats is also entered
- the seating display in the theatre is shown on the screen
- the user selects their seat(s) by highlighting the actual seats on the screen display and then clicks CONFIRM to go to the next part of the process



- the database is then searched to check the availability of the selected seats
- if the seats are available, the total price is shown + the seat numbers; this shows on another screen on the web page
- if the customer is happy with this, they select CONFIRM on the screen
- the seats are now temporarily set at NO LONGER AVAILABLE
- the customer then enters their personal details or indicates that they are a returning customer (in which case the website will already have their details)
- the payment method is then selected and payment made
- the theatre seats are then booked in the customer's name
- the final details are again shown on the screen
- an email is sent to the customer which they print out as their proof of purchase (this also acts as their printed ticket when they go to the theatre – an **e-ticket**)
- the database is finally updated with the transaction and the seats become no longer available.

Booking seats at the cinema is obviously a similar series of steps. However, booking flights is slightly more complex since it involves choosing airport, etc.

6.8.2 Flight booking systems

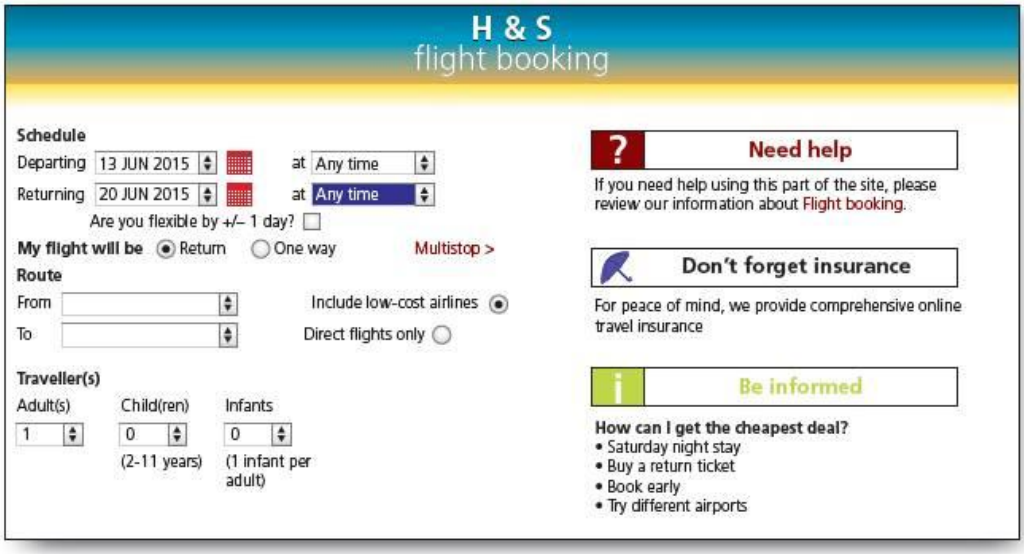


Figure 6.9 An example of an online web page for choosing flights

Exercise 6I

Using the screenshot in Figure 6.9, describe the stages when a person logs on to a flight booking website and makes a booking. Describe how the seats are booked, how double-booking is prevented, how the customer's tickets are produced and how payment is made.

Also investigate the latest ways of creating e-tickets such as Apps on smartphones and so on. Why are these new methods better than printing out a confirmation email to act as the e-ticket?

Advantages of online booking systems

- They prevent double-booking (which could happen in paper-based systems which didn't update the system fast enough).
- The customer gets immediate feedback on the availability of seats and whether or not their booking has been successful.
- The customer can make bookings at any time of the day.
- The customer's email address allows the booking company to attach 'special offers' to them and inform them of such offers automatically.
- It is usually easier to browse the seating plans (particularly on flights) to choose the best seats available at the price.
- It is possible to 'reserve' at seat for a period of time – this allows a customer to 'make up their mind' before finalising the booking of the seat (this was difficult to do with the older paper-based systems).
- Very often there are no printed tickets which saves postal costs and also allows 'impulse' bookings only a few hours in advance.
- Online booking allows the use of modern smartphone and tablet apps technology; the customer is sent a QR code which contains all the booking information necessary (this QR code is stored on the smartphone or tablet and only needs to scanned at the theatre or cinema on arrival). This removes the need to print out tickets (which can get lost) and also removes the possibility of forgeries.

Disadvantages of online booking systems

- The setting up and maintenance of online booking systems is expensive.
- All customers using this service need access to a computer and a reliable internet connection.
- It is often more difficult to cancel the booking and get your money back using online systems.
- If the server is down for maintenance or if the systems breaks down, it becomes impossible to book seats by any method (a temporary paper-based system can't be used because of the risk of double-booking occurring).
- If the websites are not well designed, it can be difficult to make exactly the booking you want or can lead you to make mistakes; this is a particular issue with flight bookings where correcting an error can cost the customer an additional fee.
- Booking online does not allow you to build a personal relationship with the travel agent who might offer free upgrades or special offers which may not be available to online bookings.

6.9 Banking applications

The use of computer technology has revolutionised how we all do our banking transactions. This section will consider:

- the use of automatic teller machines (ATMs)
- internet banking
- telephone banking
- chip and PIN technology
- clearing of cheques
- electronic funds transfer.

6.9.1 Automatic teller machines (ATMs)

Automatic teller machines (ATMs) are places where customers can get cash (or carry out certain other banking activities such as order a statement) using their credit or debit card.

The following sequence shows a typical ATM process:

Sequence for withdrawing cash	What goes on behind the scenes
Customer puts card into ATM	Contact made with bank's computer
PIN is entered using the keypad	PIN is checked to see if it is correct

A number of options are given:
• change PIN
• top up mobile phone
• see account balance
  • on screen
  • printed out
• pay in cheques
• receipt required?
• get a mini statement (e.g. transactions over the last week)
• pay a bill
• make a money transfer
• withdraw cash	

The customer selects the cash option	
A number of cash amounts are shown	Card is checked to see if card expiration date is exceeded or card is reported stolen
The customer accepts one of the options or types in a different amount	Customer's account is accessed to see if they have sufficient funds

⇨ continued...

	Check is made to see if daily limit exceeded
The customer is then asked if they want a receipt	
The card is returned	Transaction is OK
Money is dispensed	Customer's account is updated

There are a few disadvantages with ATMs:

- they are often in places where theft can take place at night
- 'bogus' ATMs can be set up to gather information about the card and retain the card
- some banks charge customers for the use of ATMs.

6.9.2 Internet banking

Using **internet banking** requires good security. It allows the transfer of sums of money between accounts, payment of bills, ordering of statements, and so on. This is of particular benefit to people who are unable to visit banks during their normal opening hours or if they suffer some disability which makes travelling to the bank difficult. Thus all the advantages of working from home are valid with internet banking. However, it is also true that the disadvantages of using the internet are very valid when applied to internet banking. As the amount of **online shopping and banking** increases, the impact on society begins to gain in significance.

Online shopping and banking means that more and more people are staying at home to buy goods and services, manage their bank accounts and book holidays etc. This would all be done using a computer connected to the internet and some form of electronic payment (usually a credit or debit card). The following notes give a comprehensive list of the advantages and disadvantages of using the internet to carry out many of these tasks.

Because there is considerable overlap between the advantages and disadvantages of online banking and online shopping, these are both considered together here (see also Section 6.13 for more information on the retail sector).

Advantages of online shopping and banking

- There is no longer a need to travel into the town centre thus reducing costs (money for fuel, bus fares, etc.) and time-wasting; it also helps to reduce town centre congestion and pollution.
- Users now have access to a worldwide market and can thus look for products that are cheaper; this is obviously less expensive and less time consuming than having to shop around by the more conventional methods; they will also have access to a much wider choice of goods.
- Disabled and elderly people can now access any shop or bank without the need to leave home which is of great benefit to them; it helps to keep them part of society since they can now do all the things taken for granted by able-bodied people.
- Because it is online, shopping and banking can be done at any time on any day of the week (i.e. 24/7) – this is particularly helpful to people who work as the shops/banks would normally be closed when they finished work.
- People can spend more time doing other things e.g. going shopping to the supermarket probably took up a lot of time; by doing this online (e.g. setting up repeat items) people are now free to do more leisure activities.
- Many people find it less embarrassing to ask for a bank loan using the internet rather than enduring a face-to-face discussion with bank staff.
- There are often long queues at the banks or checkouts at the shops, so internet banking saves time.

- The shops and banks save money by not having as many staff working for them (reduced wage bill) or hiring of high street premises (reduction in rental costs) – these savings are often passed on to customers in the form of lower interest rates, cheaper goods or higher rates on interest for savers.

Disadvantages of online shopping and banking

- There is the possibility of isolation and lack of socialisation if people stay at home to do all their shopping and banking.
- There are possible health risks associated with online shopping or banking because of a lack of exercise; if people physically go shopping then they are getting some exercise.
- Security issues are a major concern (e.g. hacking, stealing credit card details, etc.) as are viruses and other malware (e.g. phishing, pharming and so on).
- Accidentally using fraudulent bank or shopping websites is always a risk and this is linked to security issues.
- It is necessary to have a computer and to pay for the internet to take part in online shopping and banking.
- Unlike high street shopping, it is only possible to see a picture of the goods, which might not portray the exact colour of a dress for instance (nor can you try something on to see if it suits) before buying them; you also to have wait several days for the goods to arrive; returning goods is also expensive.
- High street shops and banks are closing because of the increase in online shopping or banking and this is leading to 'ghost towns' forming.
- It is easier to make errors with online banking and transfer money incorrectly to different accounts.

Effects on companies due to the spread of online shopping and banking

The earlier discussions all centred around the effects of ICT on people. Companies and other organisations have also been affected by the growth of ICT and online shopping and banking. Some of the effects are listed below:

- companies can save costs here since fewer staff need to be paid and it isn't necessary to have as many shops and banks in high streets to deal with potential customers
- because the internet is global, the potential customer base is increased
- there will be some increased costs, however, because of the need to retrain staff and the need to employ more staff in despatch departments
- there are also costs due to the setting up and maintaining of websites to enable online shopping and banking
- since there is very little or no customer–employee interaction, this could lead to a drop in customer loyalty which could lead to loss of customers (this could also be brought about by the lack of personal service associated with online shopping and banking)
- robberies are less likely due to the decrease in the number of high street banks
- banks also need to employ fewer security staff which has a cost benefit.

6.9.3 Telephone banking

Telephone banking is similar to internet banking. The main difference is that it uses the telephone rather than a computer.

With this system, the customer calls the bank using a telephone. The sequence is as follows:

- the customer keys in their account number
- they are then requested to enter a four-digit PIN or selected numbers from their PIN
- the customer will then hear various options, which might include:
  - press '1' for your balance
  - press '2' to carry out a money transfer
  - press '3' to pay a bill
  - press '4' to talk to one of our representatives
- the customer chooses one of the options (either by pressing the correct key, or some systems ask the customer to speak the number – this relies on voice recognition).

As with internet banking, customers are able to:

- check their balances anywhere in the world
- pay bills or transfer money to another account
- talk with a bank representative.

The advantages of telephone banking are similar to internet banking but with this system there is no need to have a computer and it's possible to talk to an actual human being. Many people still find this a more attractive proposition.

However, compared to internet banking, it can be much slower (there may be a long queue before you can talk to somebody) and the options can be a little more complex to navigate. But it can also be quicker if your computer isn't switched on at the time and you only want a balance enquiry.

Exercise 6m

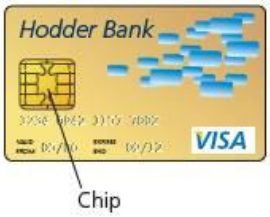
Using the notes from Sections 6.9.2 and 6.9.3, compare the advantages and disadvantages of using internet banking and telephone banking.

Consider how easy both methods are, the security issues and the need for equipment and communication lines. Also do some research and compare both methods to using banking apps on smartphones.

Put your findings into an article and try to draw some form of conclusion.

6.9.4 Chip and PIN

Many credit cards are equipped with a chip as well as a magnetic stripe – this contains key information such as the PIN.



This system is designed to enhance security since it is better than relying only on a signature. When paying for items using a chip and PIN card, a form of **electronic funds transfer (EFT)** takes place (see Section 6.9.6). In this example, suppose a customer goes into a restaurant to pay for a meal using a chip and PIN card:

1. The PIN is entered using a keypad.
2. The card is checked to see if it is valid (check on expiry date, whether stolen card, etc.).
3. The PIN is read from the chip on the card and is compared to the one just keyed in.

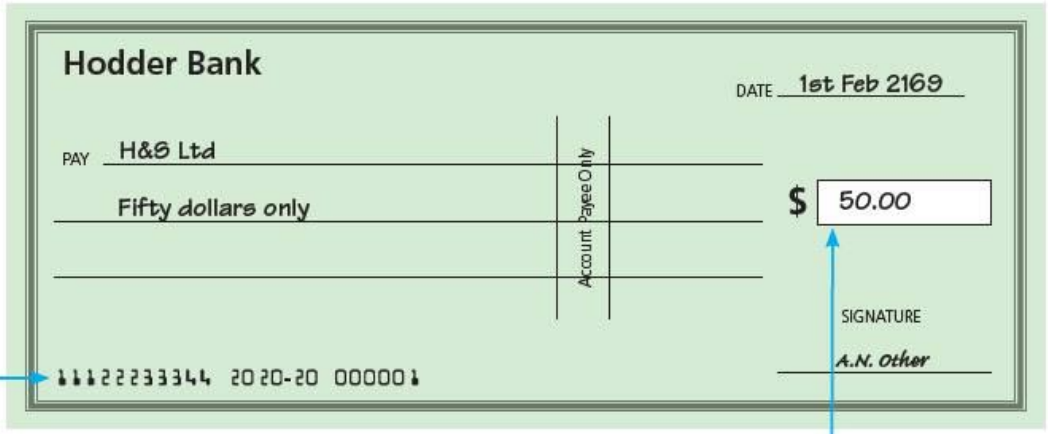
4 If they are the same, then the transaction can proceed.
If this is the third attempt at entering the PIN, then the transaction is terminated.
5 The restaurant's bank contacts the customer's bank.
6 A check is made on whether they have enough funds.
7 If the card is not valid or there aren't enough funds available, then the transaction is terminated.
8 If everything checks out OK, then the transaction is authorised.
9 An authorisation code is sent to the restaurant.
10 The price of the meal is then deducted from the customer's account.
11 The same amount of money is then added to the restaurant's bank account.
12 A receipt is produced as proof of purchase.

6.9.5 Clearing of cheques

This section reviews how banks clear cheques using a centralised clearing centre.

Suppose John uses a bank called Hodder Bank and he pays a cheque for $50 to a company called H&S Ltd who bank with the Smith Bank. How is the H&S bank account credited with $50?

First of all the cheque is sent by the Smith Bank to a centralised clearing centre. The cheque is processed by the clearing centre by first of all passing it through a reader/sorter machine. This machine automatically reads:



- the amount on the cheque
- the code line (containing account number, sort code and cheque number).

All the cheques are then sorted using their sort codes (unique, six-digit numbers that are used to identify each bank or building society), ready for sending to an exchange centre.

The data from the cheque which has been read is then converted into an encrypted file known as **IBDE (Inter-Bank Data Exchange)** file. Every IBDE is 'signed' with a digital signature so that the receiving bank can be sure that the data hasn't been tampered with.

Later, Smith Bank delivers the cheque to an exchange centre. The exchange centre then passes the cheque back to the paying bank (Hodder Bank in this case) which then sends it to its own clearing centre.

At the paying bank's clearing centre, the digital signature is first checked and then the cheque is passed through their own reader/sorter machine to make sure the data matches with that on the IBDE file. It also sorts the cheques into branch order (using the sort code).

Later on, Hodder Bank checks to see if John has enough money in his account to cover the cheque, and also that it has been signed, dated and written correctly and is genuine. Based on this information, Hodder Bank decides whether to pay John's cheque to H&S Ltd or return it unpaid to the Smith Bank.

If John's bank decides not to pay the cheque to H&S Ltd, his bank will send the unpaid cheque back to the Smith Bank by special courier.

The decision to return a cheque unpaid must be made on the morning of the day after exchange so the cheque can be returned straightaway to Smith Bank if necessary. A cheque may be returned unpaid for a number of reasons, such as:

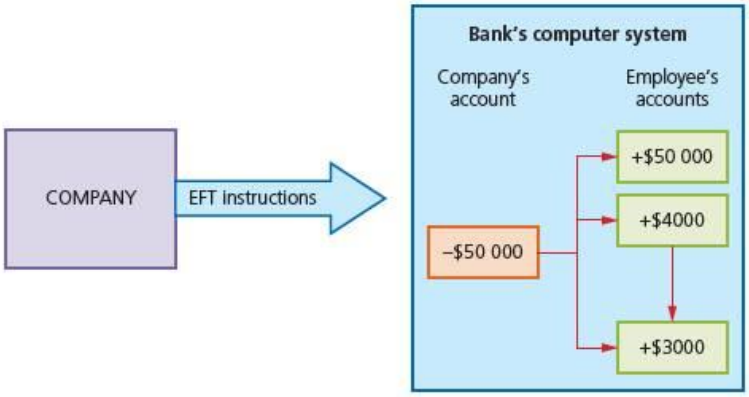
- the customer has not got enough money in their account to pay the cheque
- it has not been signed, dated, or written correctly
- it is fraudulent for some reason.

This whole process, known as 'clearing a cheque', takes three working days, so if you pay in a cheque on a Wednesday, Thursday, or Friday, it will actually take five days to clear.

6.9.6 Electronic funds transfer

Electronic funds transfer (EFT) is a system that allows money transfer instructions to be sent directly to a bank's computer system. No actual money is transferred; the whole system relies on electronic transfer of money between accounts. When an EFT instruction is received, the computer system automatically transfers the specified amount from one account to another.

One common use of EFT is the payment of salaries to the staff of a large company. On the day when payment is made, the company instructs the bank to transfer money from their account into the bank accounts of their employees.



Other examples of EFT include: When a credit/debit card is used to pay for a purchase in a store, the payment is made using a system called **Electronic Fund Transfer at Point-of-Sale (EFTPOS)**. Use of EFTPOS was discussed earlier in Chapter 2.

6.10 Expert systems

Expert systems have been developed to mimic the expertise and knowledge of an expert in a particular field. Examples include:

- diagnosing a person's illness
- diagnostics (finding faults in a car engine, finding faults on a circuit board, etc.)
- prospecting for oil and minerals

- tax and financial calculations
- strategy games (e.g. chess)
- identification of plants, animals and chemical compounds
- road scheduling for delivery vehicles.

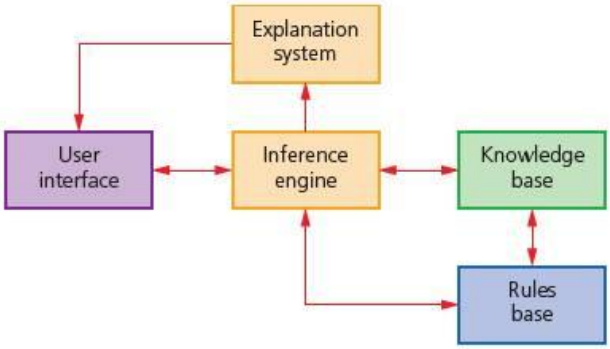


Figure 6.10 A basic expert system is made up of a number of elements

6.10.1 How to set up an expert system

- Experts in the field are interviewed.
- Data is then collected from these experts.
- A **knowledge base** is first designed and then created (the knowledge from the experts is used to populate the knowledge base).
- The **rules base** is then designed and created and an **inference engine** is also designed and created.
- An **explanation system** is also developed.
- The **input screen** and **output format** is also designed and created (this is known as the **user interface**).
- The **expert system** is tested against known conditions/scenarios and is also checked to see if it meets the original specification.
- Experts are interviewed about how effective it is before the expert system goes out on general release.

Advantages

- They provide consistent answers and are not affected by emotional reasoning.
- They never 'forget' to answer a question when determining the logic.
- Using expert systems reduces the time to solve a problem.
- They indicate the probability of the given solution being accurate or correct.
- The potential of saving money exists since there is less need for specialists (for example, when carrying out oil exploration).
- Allows areas of the world access to expertise which they couldn't normally afford.

Disadvantages

- They tend to lack common sense in some of the decision-making processes.
- Whilst lack of emotional reasoning is an advantage, it can also be a disadvantage in areas such as medical diagnosis.
- Errors in the knowledge base can lead to incorrect decisions being made.
- They are expensive to set up in the first place.
- Needs considerable training to ensure the system is used correctly by the operators.

6.10.2 Using an expert system

Using oil prospecting as an example, this is the process for using an expert system.

1. An interactive user screen appears (this is often multiple-choice questions or Yes/No responses).
2. The system asks questions about geological profiles.
3. The operator types in the answers to questions/geological profiles.
4. The system then asks questions based on the previous response(s) input by the operator.
5. The **inference engine** compares answers to questions with the facts stored in the **knowledge base** using the **rules base**.
6. The system suggests the probability of finding oil as an output.
7. It also indicates the probable depth of deposits (usually as a percentage probability).
8. The explanation system will also explain how the expert system arrived at its conclusions.
9. It will then make predictions about geological deposits in the soil/rocks.
10. Finally it will produce contour maps showing concentration of minerals, rocks, oil, etc.

Exercise 6n

1. Write a sequence of instructions to show how the following expert systems would be set up:
   - tax calculation system
   - chess
   - engine diagnostics for a racing car.
2. Write a sequence of instructions to show how the following expert systems would be used to diagnose faults or identify things:
   - circuit boards in television sets
   - identify an 'unknown' chemical compound
   - identify a new species of flower
   - produce the best route for a delivery vehicle.

6.11 Computers in medicine

Computers are used in many areas of medicine, such as:

- keeping patient records and pharmacy records
- monitoring of patients in a hospital
- diagnosis of illness using expert systems
- the use of 3-D printers in many areas of surgery.

6.11.1 Patient and pharmacy records

Doctors and hospitals need to keep accurate records of all their patients. This is essential to ensure correct diagnosis and treatment is given. An up-to-date medical history is part of the diagnosis process. Databases are kept by doctors and hospitals so that data can be shared between medical practitioners and pharmacies (e.g. to ensure no drugs are prescribed which interact with each other in an unsafe manner).

Databases also allow a quick and easy search for patient records – this could be very important in an emergency, for example, when accessing the patient's medical history could mean the difference between life and death. It also means that medication can be prescribed without issuing paper prescriptions – an email could be sent to the pharmacy.

The sort of data which would be required on a patient database is as follows:

- a unique identification number
- name and address
- date of birth
- gender (male or female)
- medical history (e.g. recent medicine/treatment)
- blood group
- any known allergies
- doctor
- any current treatment
- any current diagnosis
- important additional information such as X-rays, CT scans, and so on.

6.11.2 Monitoring patients

Note: See also Section 6.3.

By connecting a patient to a computer system, it is possible to carry out 24-hour monitoring of the patient. The computer can monitor:

- heart rate
- respiration (breathing rate)
- brain activity
- blood/body temperature
- blood pressure
- blood sugar levels
- oxygen levels in the blood.

This is not an exhaustive list, by any means.

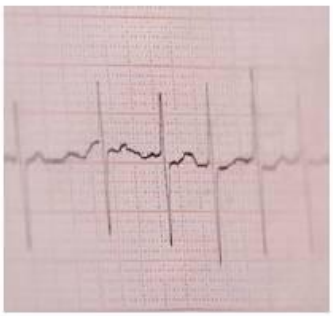


Figure 6.11 Heart beat trace

The results are shown on a monitor in the form of a digital read-out and/or graphical read-out.

Digital read-outs give the nurse or doctor an immediate value; graphical representations are used to show trends over a period of time. Both methods supply different information. There is often sound output as well in the form of beeps to indicate that the machine is working. It also indicates, for example, the heart rate and gives a warning if the patient's condition suddenly deteriorates. All of these outputs give the nurses and doctors useful information.

As discussed in Section 6.3, the system relies on sensors attached to patients and to a computer system that interprets the sensor data and converts it into a format useful to the nurses and doctors. Using sensors and computers has many advantages over taking readings manually:

- it is more accurate; using a computer system almost removes any chance of error
- they can operate 24/7 and don't require any breaks or get tired
- they never forget to take readings – a nurse could be too busy for example
- readings can be taken more frequently using computer systems
- they are capable of responding much faster to any change in the patient's condition

- they can automatically produce graphs/analyse results
- there is the potential to save money since fewer nurses need to be paid
- computers can monitor several patients at the same time
- they reduce the risk of a nurse being subjected to contagious diseases.

6.11.3 Using expert systems to diagnose patients

Expert systems were discussed in Section 6.10. One of the more common uses of expert systems is to diagnose illnesses in patients.

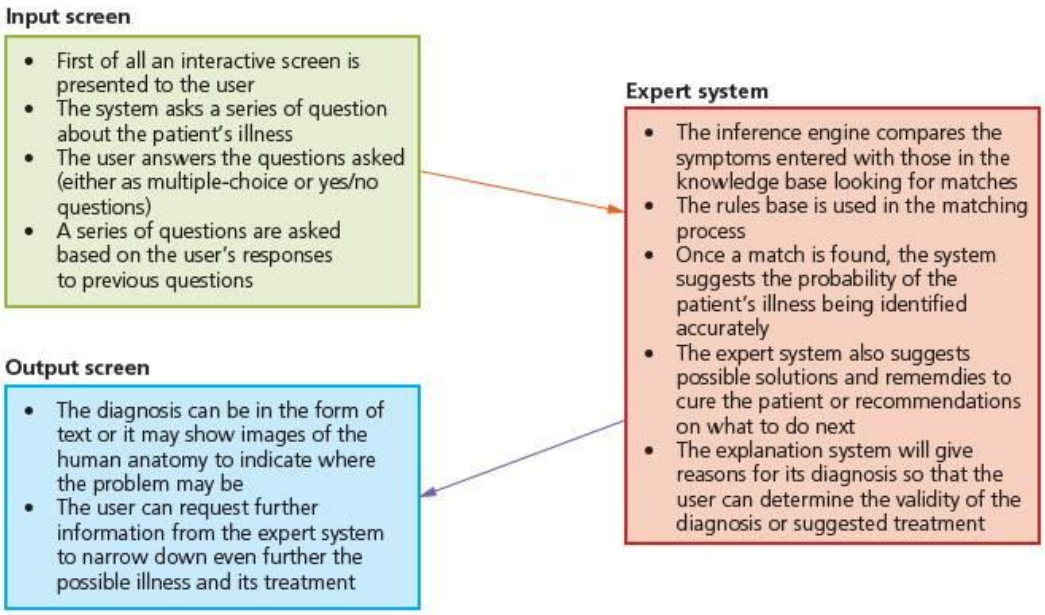


Figure 6.12 A typical patient-diagnosis expert system

6.11.4 Using 3-D printers in medicine

Chapter 2 first introduced 3-D printers. Their use in a number of fields is rapidly progressing. One of the most innovative uses is in the field of medicine. The following is just a small insight into the many developments taking place across the world.

Surgical and diagnostic aids

It is possible to print out anatomical parts using 3-D printers. These are used as an aid towards diagnosis and surgical procedures. The patient is scanned using:

- **CT** (**computed tomography** – which involves producing images of the internal parts of the body in a series of thin slices less than 0.1 mm thick)

OR

- **MRI** (**magnetic resonance imaging** – this uses strong magnetic fields and radio waves to produce a series of images of the internal organs in the body).

A 3-D printer can then reproduce a solid object showing the exact internal organs of the patient. The doctor or surgeon can then show the patient exactly what is wrong and then show them what procedures are required. They also help the surgeons in planning surgical procedures since they can see exactly what is required well in advance of the operation.

3-D printing systems enable blood vessels, major arteries, tumours and so on to be part of the diagnostic, pre-surgical aids. This also allows for patient engagement which would be missing from the more traditional consultation methods.

Some 3-D printers produce hard nylon objects which are used in certain pre-surgical planning. If a patient has suffered a bone break, for example, surgeons can physically test and position screws and plates in the '3-D bone nylon image' prior to the surgery taking place. This reduces the chance of any errors when the actual procedure is carried out.

Prosthetics

3-D printers are now being used to print out prosthetics (false arms, hands and legs). Whilst state-of-the-art myoelectric prosthetics cost tens of thousands of dollars, the price for 3-D printing a prosthetic arm or hand can be as little as $100.

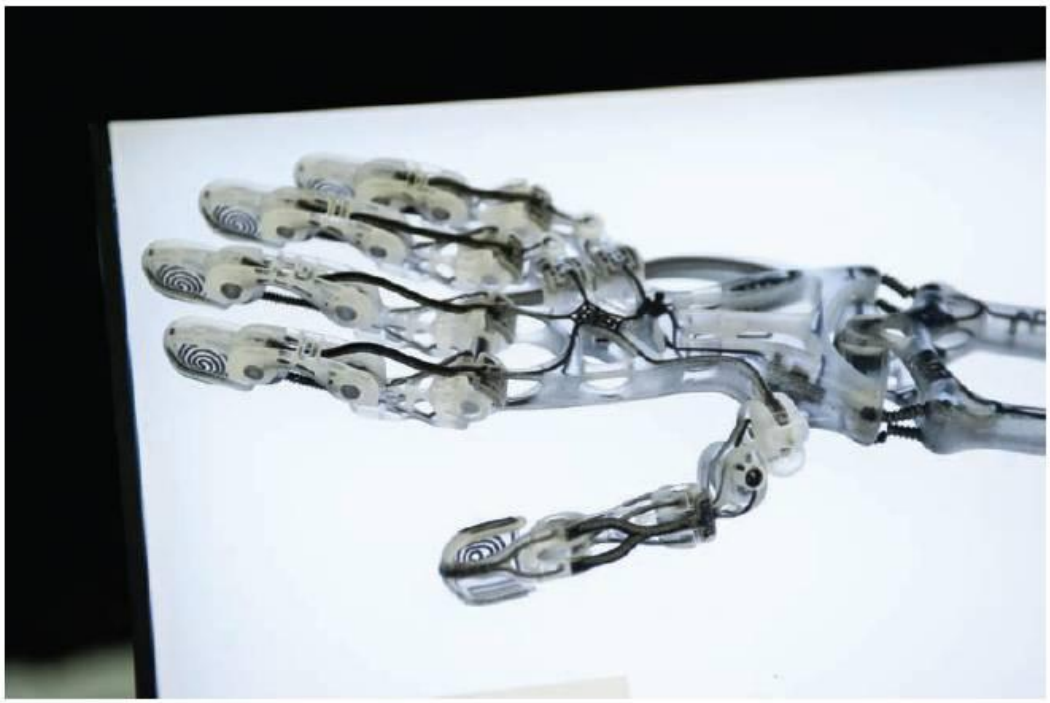


Figure 6.13 This image shows a prosthetic arm produced by a 3-D printer. Whilst the technology may not be cutting-edge, it can be life-changing to an amputee.

There is still much research needed in this field. However, the results to date are very encouraging with many more people from poorer countries now having a chance to replace missing limbs at a fraction of the cost compared to existing methods.

Tissue engineering

Recent advances have allowed the 3-D printing of bio-compatible materials, cells and supporting structures. This has improved the viability of the function of cells within a 3-D printed object. 3-D bio-printing is a very complex process and requires the input from biologists, medical engineers, physicists and other engineers. It has already been used successfully to produce multilayered skin tissue, bone tissue, heart/artery grafts and tracheal splints.

The procedure involves making biological materials by diffusing cells into a bio-compatible scaffold. The bio-printed tissue is then put into an incubator and the cell structure held within the scaffold grows to form actual cellular tissue.

There is still much research to do, but the goal of growing replacement organs, using cells from the actual patient, is getting ever closer thanks to 3-D printing technology.

Design of medical tools and equipment

3-D printers are now being used as part of the product development cycle for medical tools. This allows new medical equipment/tools to be made ready for the market much faster. Traditional methods of producing new equipment/tools are very time consuming and very expensive. 3-D printers create injection-moulding tools which allow several prototypes to be made within a short period of time. Traditional methods require aluminium moulds to be made which is a slow and expensive process. Development time is reduced, on average, by up to 90% and development cost is reduced, on average, by up to 70%. This is important in the field of medicine where it is essential that development time and costs are reduced to a minimum.

6.12 Computers in libraries

Many library systems are now computer-controlled. They usually involve the use of barcodes on the books being borrowed and on the borrower's library card. The following describes a type of computerised library system based on barcodes.

1 Two files will exist containing:
Book file (this contains a number of records made up of the following fields):

Barcode	Book title	Name of author	Date published	Unique book identifier	Borrower's ID

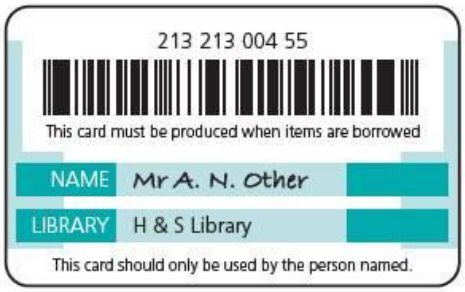
Borrower's file (this contains a number of records made up of the following fields):

Borrower's ID	Borrower's name	Borrower's details	Barcode of book borrowed	Unique book identifier	Date due back

2 Thus, when a borrower takes out a book, the barcode is first of all scanned.

- The book details are then found on the book file.
- The system automatically calculates the 'due back' date based on the day the book is taken out.

3 The borrower's library card contains a unique barcode which is then scanned.



- The book file is linked to the borrower's file and both files are updated to indicate which book has been borrowed and when it is due back.
- The date the book is due back is saved in the borrower's file. The system therefore knows when to send out a reminder to the borrower of the book if the return date of the book is exceeded.

4 On a daily basis, the borrower's file is interrogated by the computer to see which books are overdue for return. The sequence of events is summarised below:
- the computer reads a record from the book file
- the corresponding record is read from the borrower's file
- it compares the due date back with the current date
- the borrower details are then found and a letter or email is automatically sent out
- the next record in the book file is then read
- and so on until the whole file has been checked.

Barcodes are not the only way of tracking books borrowed from a library. Some systems use magnetic stripes on the borrower's cards rather than barcodes. The procedure is the same except the card is now passed a magnetic card reader rather than being scanned. The borrower's data and book data are still connected as described above. Some libraries use RFID chips in their books.

6.13 Computers in the retail industry

6.13.1 Automatic stock control system using barcodes

Barcodes now appear on most products sold in shops; they allow quick identification of product details once the barcode has been scanned by a **barcode reader**. Supermarkets, in particular, use **electronic point of sale (EPOS) terminals** which incorporate a barcode reader which scans the barcode and retrieves the price of the article and also relays information back to the computer system allowing it to update its files (more of this later).

Figure 6.14 Barcodes are made up of alternating dark and light lines of varying thickness

A number underneath the barcode usually consists of four parts: a country code, manufacturer's code, product code and a check digit. The check digit is a form of **validation** which is used to make sure no errors occurred during the reading of the barcode.

Barcodes are used in the following applications:

- library book system (see Section 6.12)
- administration systems
- passport/ID cards
- some burglar alarm systems
- equipment checking systems (safety records on maintenance of equipment)
- automatic stock control systems.

The following description is a detailed account of how barcodes are used to automatically control stock levels in a supermarket.

- Barcodes are attached to all items sold by the supermarket.
- Each barcode is associated with a stock file which contains details such as price, stock levels, product description – the barcode will act as the primary key in the file.
- A customer takes their trolley/basket to the EPOS terminal once they have completed their shopping.

- The barcode on each item is scanned at the EPOS.
  - If the barcode can't be read, then the EPOS operator has to key in the number manually.
- The barcode is searched for on the stock file record by record until a match is found.
- Once the barcode has been found, the appropriate record is accessed.
- The price of the item is then found and sent back to the EPOS together with a product description.
- The stock level for the item is found in the record and is reduced by 1 and the new stock level is written back to the file.
  - If the number in stock of the item is less than or equal to the re-order/minimum number in stock, then the computer automatically orders a batch of items from the suppliers (supplier information would be found on another file called the order file or supplier file – the barcode would be the link between the two files).
  - Once goods have been ordered the item is flagged on the file to indicate an order has been placed; this now prevents re-order action being triggered every time this item is scanned until the new stock arrives.
  - When new goods arrive, the barcodes on the cartons will be used to update the stock files; also any flags associated with these goods will be removed so that the stock checks can start to be made again.
- The above procedure is repeated until all the items in the customer's basket/trolley have been scanned.
- When all the items have been scanned, the customer is given an **itemised bill** showing a list (with prices) of everything they have bought.
- The computer also updates the files containing the daily takings.
- If the customer has a loyalty card, the system will also automatically update their points total.

Some newer supermarkets now allow customers to scan their own items at special checkouts; these basically work the same way as the normal EPOS terminals.

Other retailers use a similar system with only minor differences.

6.13.2 Electronic funds transfer and chip and PIN cards

How electronic funds transfer and chip and PIN cards are used in the retail industry have already been fully described in Section 6.9.

6.13.3 Internet shopping

A discussion on internet shopping, including its advantages and disadvantages, was fully covered in Section 6.9 and won't be repeated here.

Exercise 6o

1 Revisit the earlier sections of this chapter and other parts of the book. Gather together your information and then write an article on the advantages and disadvantages of shopping on the internet compared to shopping on the high street.

Consider aspects such as convenience, costs and security when writing the article.

2 Find out as many areas in the retail industry that use barcodes (including QR codes) and explain why barcodes are used. What other methods exist which could replace barcodes? Why have these other methods not been adopted?

6.14 Recognition systems

6.14.1 MICR, OCR, OMR and RFID

The operation of MICR, OCR, OMR and RFID was discussed in detail in Chapter 2. However, the following additional notes on two uses of OMR are worth studying.

School registers

Newer methods of registering students were mentioned earlier on in this chapter (i.e. use of magnetic stripe cards and biometrics). However, paper-based systems are still used in some schools. These paper-based registers are often scanned in to a computer using OMR. The attendance records are then stored on a central database.

FIRE Academy

Term 1 Week 4 (2016)
Tutor Group: 7AS

	Monday		Tuesday		Wednesday		Thursday		Friday	
Init	am	pm	am	pm	am	pm	am	pm	am	pm
AA										
RC										
FD										
AE										
BE										
HK										
TL										
SM										
AN										
LN										
AP										
AR										
SW										

The database can be searched or sorted for the data about the attendance of any student.

Multiple-choice question (MCQ) papers

Completed multiple-choice forms are scanned in using OMR. The forms have timing marks down one side – these timing marks pass under the first column sensor of the scanner. These marks indicate the position of each question on the paper. Using OMR software, a template is created to map out the X–Y coordinates of each lozenge (area which is filled in by pencil/ink or left blank) – a value is then assigned to each lozenge. As each MCQ is scanned, a light passes through the scanner which picks up the position of each lozenge which has been filled in by pencil/ink. The position of the filled in lozenges is compared to the corresponding coordinates on the 'answer sheet template'. If the position matches to the X–Y coordinates, then the answer is recorded as being correct. The scanned results are exported to a database or spreadsheet.

If more than one lozenge is filled in for each question, then the OMR software simply discards that result. Marking MCQ sheets using OMR is much quicker and more accurate than doing the task manually. Because the results are automatically exported to a database or spreadsheet, it is much easier to analyse the results.

6.14.2 Automatic Number Plate Recognition (ANPR) System

Automatic number plate recognition (ANPR) systems are used to read the number plates on cars in a number of applications.

In the example that follows, we will describe how ANPR is used in a car park to enable entry and exit to be automatically controlled by a computer system.

Step 1

A sensor detects a vehicle and sends a signal to a microprocessor to instruct a camera to capture an image of the front of the vehicle (often an infrared camera is used to give a clearer image and for use at night).

Step 2

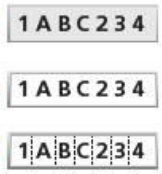
i An algorithm is used to locate and isolate the number plate from the image taken by the camera. This algorithm also takes into account the size of the number plate and any damage or orientation.

ii The brightness and contrast of the number plate is first adjusted (this ensures that the characters can be clearly read).

Each character on the number plate is then segmented

iii Each character is then recognised using optical character recognition (OCR) software. The characters are converted into a string of editable text by the software.

iv This text string is then stored on a database.



Step 3

Once all of this has happened, the car park barrier is raised and the motorist is issued with a ticket. The ticket shows the date and time of entering the car park.

Step 4

When the motorist returns to the car park, they insert their ticket into a machine which calculates the car park charges. The payment is registered on the database.

The motorist then drives to the exit barrier and the ANPR system again reads the number plate and checks its database. If the number plate is recognised (and payment has been made), the exit barrier is raised.

Exercise 6p

Do some research to find out other applications of ANPR.

Write down the advantages and disadvantages of ANPR for each application that you find.

6.15 Monitoring and tracking systems

6.15.1 Monitoring/tracking a member of the public

There are a number of reasons why a person may need to be tracked:

- the person may be an offender who is released from prison on the understanding that their whereabouts is known at all times
- an elderly person may need to be tracked to ensure their safety
- it may be necessary to track somebody taking part in a marathon to determine their position and their time to complete the race.

Other applications will exist.

An ankle monitor makes use of RFID technology by inserting a microchip into the device which is strapped to the ankle.

It sends out (at timed intervals) radio frequency signals. These signals contain the person's location and other data. They are tamper-proof devices and automatically alert the authorities if an attempt is made to remove the monitor from the ankle.

Figure 6.15 An ankle monitor

The monitor sends out RF signals which are picked up by a device in the person's home. This unit uses either landline or mobile phone networks to relay the information back to a computer in a control room. If the person isn't at home at an agreed time, an alert is sent to the control room. GPS (see next section) monitoring is also used so that the person can be tracked outside their home. This allows the exact location of the person to be known at all times. The GPS system works by sending signals to a mobile phone which the person must carry with them at all times. CCTV cameras are also used to monitor people in streets and shopping malls in case of crime or any suspect activity.

6.15.2 Cookies

Please refer to Chapter 8 for notes on how cookies are used to keep track of a person's buying habits when using the internet.

6.15.3 Key logging

Key-logging software is covered in Chapter 8. This software is used to monitor each key press on a user's computer. The key presses are sent back to the person who installed the software on the user's computer.

6.15.4 Employee call monitors

Employee call monitoring allows managers to listen in to employees' telephone calls for the following reasons:

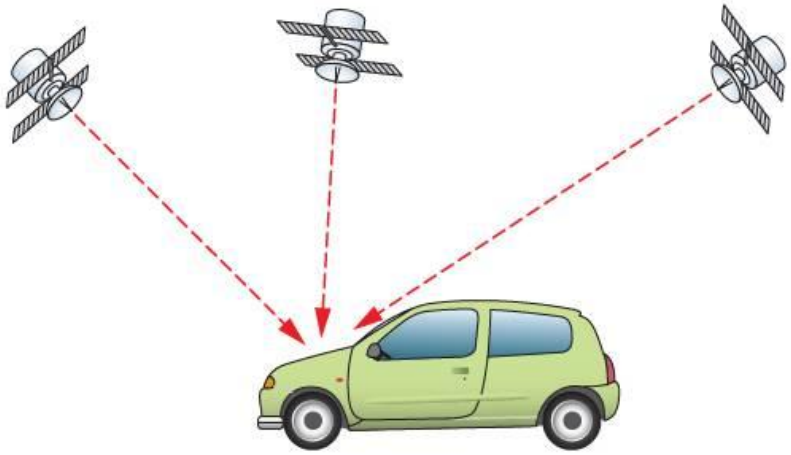
- to improve the employees performance (e.g. at a call centre)
- allows the manager/supervisor to join in a call where necessary
- can be used as a training tool
- it allows a company who are concerned about security to monitor all calls
- if the workforce move around, it can be used to make sure they correctly represent the company whilst out of the office.

There are three types of call monitoring:

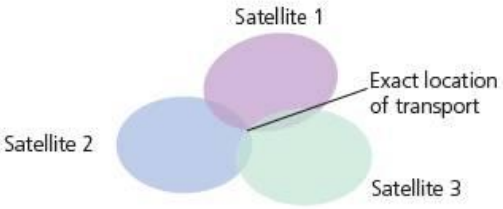
1 **monitor**: this allows the manager/supervisor to listen in on calls (the line is muted so that neither the employee or the other person being called is aware of their presence)
2 **whisper**: this allows the manager to speak to employees to help them with a call (only the employee can hear the manager/supervisor's voice
3 **barge**: this allows the manager/supervisor to be heard by both the employee and the other person in the call).

6.16 Satellite systems

6.16.1 Global positioning satellite (GPS) systems and satellite navigation

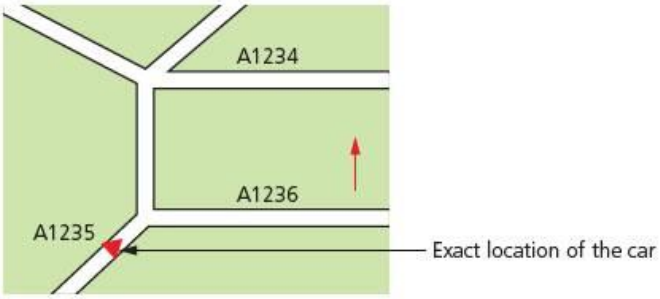


Global positioning satellite (GPS) systems are used to determine the exact location of a number of modes of transport (e.g. airplanes, cars, ships, etc.). Cars usually refer to GPS as **satellite navigation systems** (i.e. satnav).



Satellites surrounding the Earth transmit signals to the surface. Computers installed in the mode of transport receive and interpret these signals. Knowing their position on the Earth depends on very accurate timing (atomic clocks are used in the satellites which are accurate to within a fraction of a second per day). Each satellite transmits data indicating its position and time. The computer on board the mode of transport calculates its exact position based on the information from at least three satellites.

In cars, the onboard computer contains stored road maps. With these satnav systems, the car's exact location, based on satellite positioning, can be shown on the map and the driver can also be given verbal instructions such as: 'After 100 metres, take the next left turn onto the A1234'. A screen on the satnav device will also show the car's position in relation to the road network.



Advantages

- The driver doesn't have to consult paper maps, so it is far safer.
- It removes errors (can warn drivers about one way streets, street closures, etc.).
- The system can warn the driver about the location of speed cameras (again aiding safety).
- The system can estimate the time of arrival.
- It is also possible to program in the fastest route, route to avoid towns, etc.
- The system can also give useful information such as location of petrol stations.

Disadvantages

- If the maps are not kept up to date, they can give incorrect instructions.
- Unless the system is sophisticated, road closures, due to accidents or road works, can cause problems.
- Loss of satellite signals can cause problems.
- If an incorrect start point or end point is keyed in the system will give incorrect information.

6.16.2 Geographic information system (GIS)

Geographic information system (GIS) is a computer system that allows us to map, model, query and analyse large amounts of data according to their location.

GIS allows users to create interactive queries, analyse spatial information (this refers to how objects fit together in space) or edit map data. The technology combines maps with computer graphics and databases.

Essentially GIS enables the following:

- amalgamation of information into easily understood maps
- performance of complex analytical calculations and then presentation of the results in the form of maps, tables or graphics (or a combination of all three)
- geographers, scientists and engineers are able to see the data in several different ways in order to see patterns and relationships.

The following example shows how these **layering** techniques are used to produce a visually effective answer to a query made in the GIS system.

Carrying out queries on GIS systems (in a method similar to internet searches) will produce the data which matches the query. The data will be displayed in the form of a diagram, map or set of tables. By zooming into the map, it is possible to find finer details about the layering data used.

Uses

- Emergency services use GIS to send the closest emergency personnel to a location.
- Biologists and environmentalists use GIS to protect animal life and plants in certain vulnerable areas (which meet a certain criteria after carrying out a search on the database).
- Teachers can use GIS in their geography, science or engineering lessons.

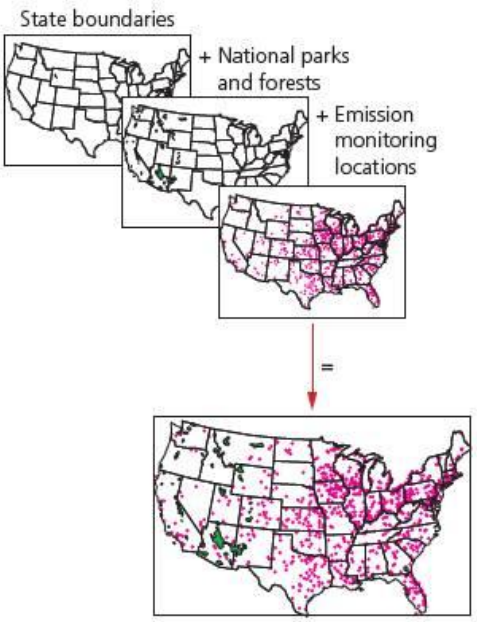


Figure 6.16 Layering state boundaries with national parks and emission monitoring stations produces the final map shown

6.16.3 Media communication systems

Communication media refers to methods of delivering and receiving data/information using telecommunications.

There are many media used to send and receive information (e.g. fibreoptics, copper cable and Wi-Fi); we will concentrate on the global communication method which makes use of satellites.

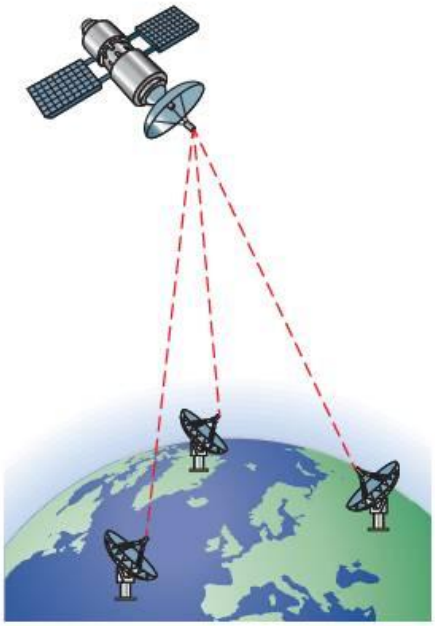
Satellites contain antennas, transponders (to allow receiving and sending of data), solar panels (for power from the Sun) and propulsion (to ensure the satellite is in the correct orbit at all times).

Signals are converted to analogue (if necessary) and then beamed to the satellite from a satellite dish on Earth. The signals are delivered by carrier waves which consist of radio waves. Each signal has its own frequency and bandwidth (the larger the bandwidth the more data can be transmitted).

Once the data reaches the satellite it is then resent to Earth. The satellite usually 'boosts' the signal before sending it back to Earth. Often the frequency is changed to prevent the signal received being confused with the signal sent.

The satellite system is used to transmit data from one part of the planet to another. Due to the often great distances, cables would be too costly and there is also the problem of signal deterioration over long distances.

Satellites systems are used to transmit television, telephone and internet data around the world.



7 Systems life cycle

In this chapter you will learn about:

- systems analysis, including:
  - analysis stage
  - design stage
  - development and testing stage
  - implementation stage
  - documentation
  - evaluation stage.

A systems analysis team is often brought in to review an existing system and suggest a number of improvements. The existing method used may be either a manual, paper-based system, or, more usually, it could already be a computer-based operation that is no longer regarded as adequate for the task.

There are many stages in systems analysis, which are covered in Sections 7.1 to 7.6.

The main stages in the systems life cycle can be summarised as shown in Figure 7.1.

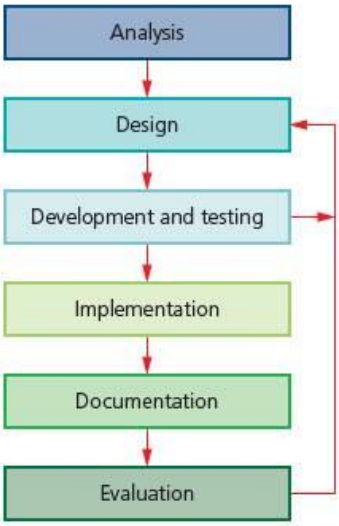


Figure 7.1 The stages in the systems life cycle

7.1 Analysis

The basic steps in the **analysis** stage can be summarised as shown in Figure 7.2.

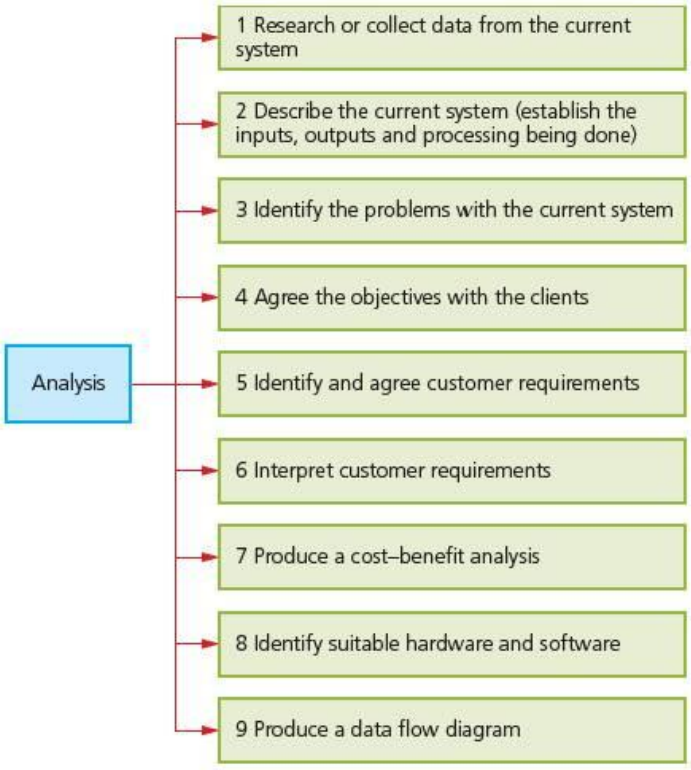


Figure 7.2 Analysis stages

Stages 2 to 8 in Figure 7.3 are sometimes referred to as the **feasibility study** and this can be further broken down as follows:

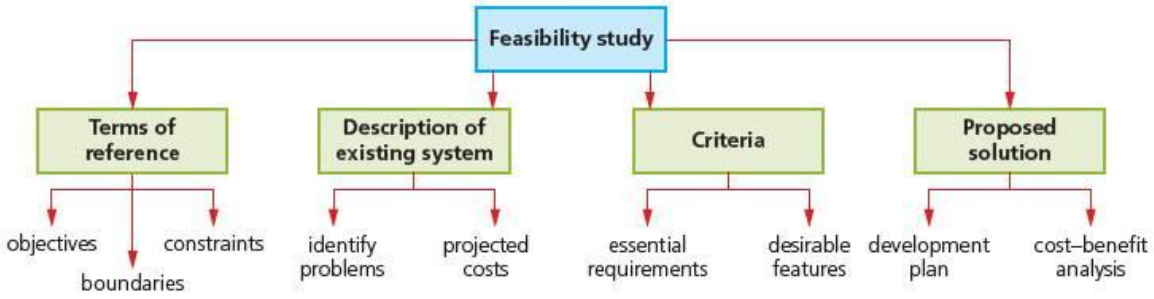


Figure 7.3 Feasibility study stages

We will now consider the first item in the analysis stage – **researching an existing system**. There are four common methods used in fact finding, which have been summarised in Table 7.1 below. The methods are:

- **observation**
- **questionnaires**
- **interviews**, and
- **looking at existing paperwork**.

Table 7.1 Methods of research

Name of research method	Description of research method	Advantages of method	Disadvantages of method
Observation	This method involves watching personnel using the existing system to find out exactly how it works	• the analyst obtains reliable data • it is possible to possible to get an overall view of the system • a relatively inexpensive method	• people are generally uncomfortable being watched and may work in a different way • if workers perform tasks that contravene standard procedures, they may not do this while being watched
Questionnaires	This method involves distributing questionnaires to the workforce, clients or system users to find out their views of the existing system and to find out how some of the key tasks are carried out	• the questions can be answered quite quickly • it is a relatively inexpensive method • individuals can remain anonymous if they want • this method allows quick analysis of the data	• the number of returned questionnaires is often low • the questions are rather inflexible since they have to be generic • there is no immediate way to clarify a vague or incomplete answer to a question
Interviews	This method involves a one-to-one question-and-answer session between the analyst and the employee/customer. It is a good method if the analyst wants to probe deeply into one specific aspect of the existing system	• it gives the opportunity to motivate the interviewee into giving open and honest answers to the analyst's questions • the method allows the analyst to probe for more feedback from the interviewee (it is easier to extend a question) • it is possible to modify questions as the interview proceeds and ask questions specific to the interviewee	• it can be a rather time-consuming exercise • it is relatively expensive (use of analyst's time) • the interviewee can't remain anonymous with this method
Looking at existing paperwork	This method allows the analyst to see how the paper files are kept, look at operating instructions and training manuals, check the accounts, etc. It allows the analyst to get some idea of the scale of the problem, memory size requirements, type of input/output devices needed, etc.	• this method allows information to be obtained which wasn't possible by any of the other methods • analysts can see for themselves how the paper system operates	• it can be a very time-consuming exercise • because of the analyst's time needed, it is a relatively expensive method to use

In Figure 7.2, one of the stages mentioned was the production of a **data flow diagram (DFD)**. DFDs help the analyst by showing the data flows, input and output requirements, processing and the types of data storage needed.

Figure 7.4 shows a type of DFD. The example given covers reserving a seat on a flight – it shows how the data flows from stage to stage, the inputs and outputs, any processing done, and storage (booking system – most likely to be a database stored on a hard disk drive).

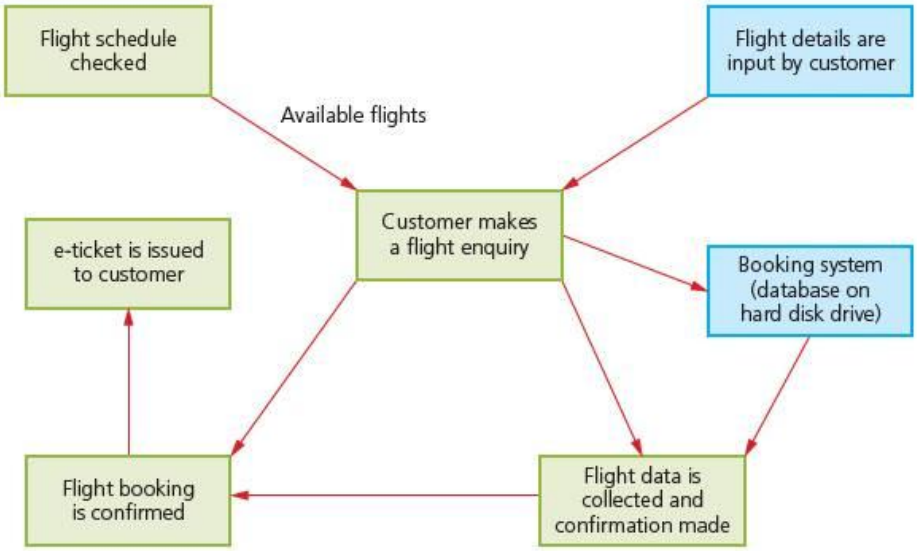


Figure 7.4 Data flow diagram (booking a flight)

Exercise 7a

The data flow diagram shown in Figure 7.4 is one example of the symbols that can be used. Research alternative methods of showing DFDs, and then redo Exercise 6l (page 110) on booking a flight using the alternative DFD symbols you have found.

DFDs in general are used to describe:

- the need to identify inputs, outputs and processing of the current system
- the need to identify problems with the current system
- the need to identify the user and information requirements for the new system
- system specifications:
  - identify and justify suitable hardware for the new system
  - identify and justify new software for the new system.

7.2 Design

Once the analysis has taken place and the systems analyst has some idea of the scale of the problem and what needs to be done, the next stage is to **design** the key parts of the recommended system. A list of tasks is summarised in Figure 7.5, but it is by no means exhaustive.

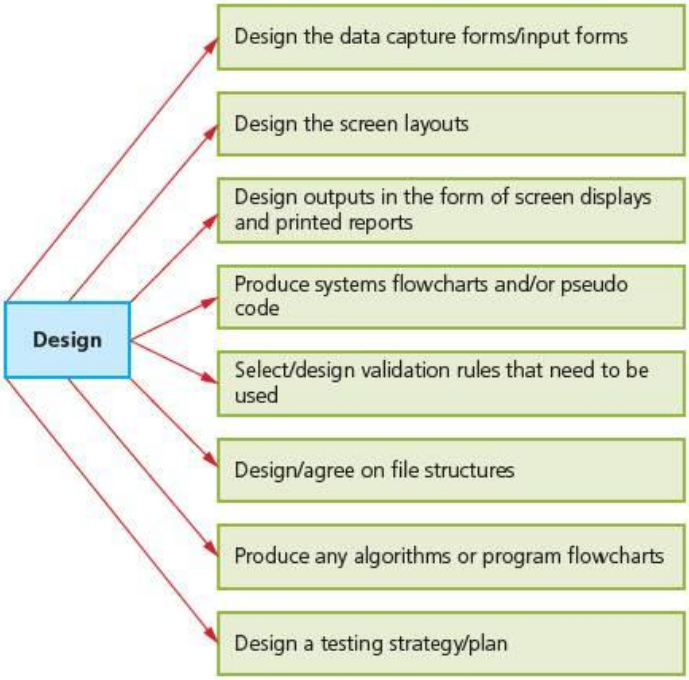


Figure 7.5 Design stage tasks

We will now consider in more depth some of these tasks listed in the design stage.

7.2.1 Data capture forms

These forms allow the data to be input into the system. They will be either paper-based or electronic-based depending on the application.

Paper-based forms need to:

- have a heading to make the purpose of the form clear
- make it clear to the person filling in the form where they must place their answers
- make use of text boxes, which will limit the amount of information collected
- make use of character boxes for data such as surnames, telephone numbers, and so on (each box allows one character only)
- make use of printed text boxes to allow for easy input of items such as date of birth
- make use of tick boxes to make choices easier (such as sex – male or female)
- make sure there is sufficient space to write answers
- use clear fonts and clear text colours to ensure the form is easy to read.

Figure 7.6 shows a typical example, which allows data about a car for sale to be manually completed for later input into a computer database.

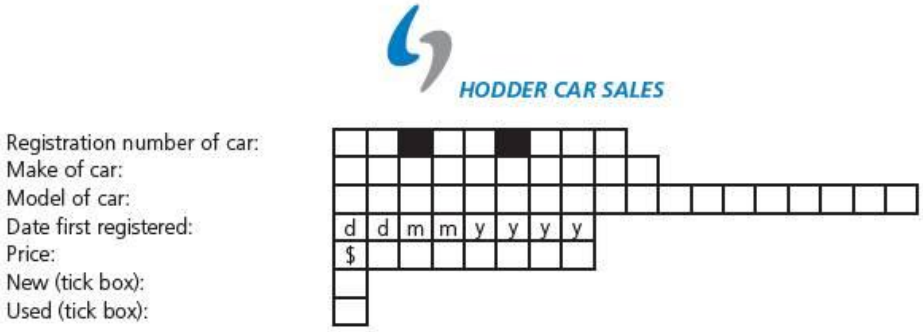


Figure 7.6 Paper-based data capture form

A computer-based data capture form is slightly different. These often have the following features:

- use of text boxes to capture key data clearly
- use of on-screen help when completing the form
- use of drop-down/combo boxes where there are limited choices
- use of radio buttons and tick boxes, requiring a single click of a mouse to select
- automatic validation of data as it is entered
- control buttons (such as next form, clear entry, save, etc.)
- double entry boxes (with verification rules) to check correctness of key data (for example, when keying in an email address).

In the car sales example shown above, the following differences could be used with a computer-based data capture form:

- **registration number**: same as paper-based form
- **make of car**: make use of a drop-down box as there is a limited number of manufacturers
- **model of car**: same as paper-based form
- **date first registered**: use of drop-down boxes for day, month and year
- **price**: use boxes as shown but include a validation check
- **new or used**: use of tick box or radio button to indicate option
- **other features**: a back and forward button (to complete details of all cars), and a save button when form is complete for each car.

Exercise 7b

Design a computer-based data capture form using the fields given above. Remember that it has to be completed online, so it should include radio buttons, drop-down boxes and so on. It should look a little different to the paper-based form shown in Figure 7.6.

7.2.2 Screen displays and printed reports

The output from any system needs careful consideration since this is part of any user interface and is also the result of some form of processing. Screen outputs should be designed:

- to make sure the size of all the output fields is correct
- so that any instructions/descriptions are clear
- so that the full screen is utilised (avoiding large areas of 'nothing')
- so that colours and fonts (size and type) make the output clear.

Figure 7.7 Screen output example

If the output is on paper then consideration must also be given to the type of output. Items such as headers and footers, fitting the page correctly, whether it should be in colour, and so on, all have to be carefully planned.

Reports (often the output from a database search) should clearly show all the fields that were included in the search criteria – output is usually in the form of a table (the example in Figure 7.8 outputs a list of all sales managers aged over 40).

Employees

Last Name	First Names	Job Title	Business Phone	Address
Pitt	Michael	Sales Manager	001 234 1235	2nd Avenue
Hawkin	Jason	Sales Manager	001 235 1245	4th Avenue
Amin	Manjit	Sales Manager	001 222 3456	9th Avenue
Clark	Katie	Sales Manager	001 234 1119	2nd Avenue
Fawkler	Jemima	Sales Manager	001 299 8745	11th Avenue

Figure 7.8 Report example

7.2.3 System flowcharts

System flowcharts are used to show how data flows through a system and also how decisions are made. They make use of special symbols that represent input/output, processing, decisions and data storage.

Systems analysts use these charts to give an overall view of the proposed system. They don't form the basis of a flowchart from which software can be written but they do show how the processes are carried out and where various hardware devices are used in the system. A sample system flowchart is shown in Figure 7.9 (this is just part of an overall system flowchart showing the flight booking system again).

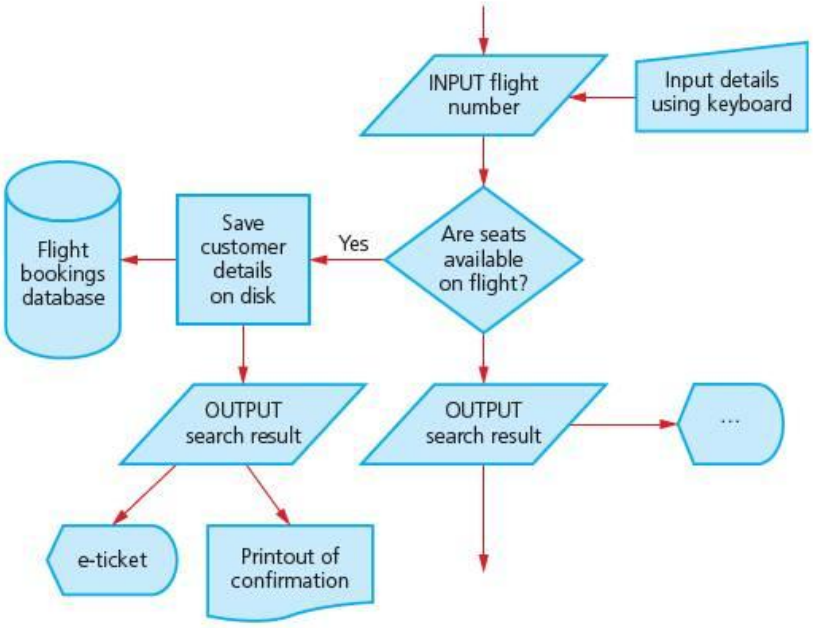


Figure 7.9 Sample system flowchart

7.2.4 Verification

Verification is a way of preventing errors when data is copied from one medium to another (for example, from paper to disk/CD). There are two common ways that verification checks are carried out.

- **Double entry**: in this method, data is entered **twice**, using two people, and is then compared (either after data entry or during the data-entry process).
- **Visual check**: this is the checking for errors by the person who is entering the data; they compare the entered data with the original document (i.e., what is on the screen is compared to the data on the original paper documents – note that this is **not** the same as proofreading).

7.2.5 Validation

Validation is a process where data is checked to see if it satisfies certain criteria when input into a computer; for example, to see if the data falls within accepted boundaries. A number of validation techniques exist; Table 7.2 highlights some of the more common checks used when writing computer software.

Table 7.2 Validation checks

Validation check	Description	Example(s) and comments
Range check	checks whether data is within given/ acceptable values	e.g. to check if a person's age is > 0 but is also < 150
Look-up check	this checks whether the data entered exists and is stored in a table of data	e.g. check is 'senior manager' exists as on option in the query such as: 'PLEASE ENTER YOUR JOB TITLE'
Length check	checks if the input data contains the required number of characters	e.g. if a field needs six digits then inputting a five-digit or seven-digit number, for example, should cause an error message
Character/type check	checks that the input data doesn't contain invalid characters	e.g. a person's name shouldn't contain any numbers, but a person's height should only contain digits

⇨ continued...

Format/picture check	checks that data is in a specific format	e.g. date should be in the form dd/mm/yyyy e.g. xnnnn which shows a person's identification (a single letter followed by five digits)
Presence check	checks if data is actually present and hasn't been missed out	e.g. in an electronic form a person's telephone number may be a required field so, if no data is entered, this should give rise to an error message
Consistency check	checks if fields correspond (tie up) with each other	e.g. if 'Mr' has been typed into a field called 'TITLE' then the 'GENDER' field must contain either 'M' or 'Male'
Check digit	this is an extra digit added to a number which is calculated from the digits (refer to Sections 6.12 and 6.13)	check digits can identify three types of error: • if two digits have been transposed during input e.g., 13597 instead of 13579 • an incorrect digit entered twice, e.g., 13559 in instead of 13579 • a digit missed out altogether, e.g., 1359 instead of 13579

7.2.6 File structures

Designing and agreeing file structures is an important part of the design stage. The fields used in the files need to take the following into account:

- field length
- field name (suitable names should be chosen)
- data type.

A **data dictionary** is used to show suitable field names. An example of a data dictionary is given in Table 7.3.

Table 7.3 Example of a data dictionary

Field name	Field length	Field type	Suitable validation check
product_code	8	alphanumeric	length check
manufacture_year	4	numeric	range check
product_name	20	alphanumeric	none
location_of_stock	4	numeric	character check
colour	2	alphanumeric	look-up check

7.2.7 Design and testing strategy/plan

When producing the software for the new system, it is very important to test it thoroughly in order to:

- make sure it meets the agreed client requirements
- remove any bugs/errors from the system
- make sure it produces the required output for data where the correct output is already known
- check that the software doesn't crash under certain conditions.

To do this, it is necessary to produce a testing strategy or plan to ensure all the possible scenarios have been tested so that the criteria have been met. Refer to Section 7.3.2 for more information on this topic.

7.3 Development and testing

7.3.1 Development

Once the design stage is completed, it is then necessary to create the system and test it fully. This section considers some of the development stages and testing strategies that are often adopted by systems analysts.

- If the system contains files (for example, a database) then the file structure would need to be finalised at this stage (e.g. what type of data is being stored in each field, length of each field, decide on which field will be the key field, how will the data files be linked, etc.). Once the file structure has been determined it is then created and tested fully to make sure it is robust when the system actually goes live.
- Since it is important that the correct data is stored in files (etc.) there are certain techniques that need to be adopted to make sure the data populating the files/database is at least of the right type and that it conforms to certain rules. Validation routines and verification methods are used to ensure this happens. Again, these routines have to be fully tested to ensure they do trap unwanted data but also to make sure that any data transferred from a paper-based system to an electronic system has been done accurately.
- Obviously any system being developed will have some form of user interface. The types of hardware have already been considered; how these are used to actually interface with the final system now needs to be identified. For example, how the screens (and any other input devices) will be used to collect the data and the way the output will be presented. If specialist hardware is needed (for example, for people with disabilities) then it will be necessary to finalise how these devices are used with the system when it is implemented. This will be followed by thorough testing to ensure that the user screens are user-friendly and that the correct output is associated with the inputs to the system.

7.3.2 Testing strategies

Software is often developed in **modular** form. This method allows the software to be broken down into smaller parts (known as modules). Each part is developed separately by a programmer (or team of programmers) and is then tested to see if it functions correctly. Any problems resulting from the testing require the module to be modified and then tested again.

Once the development of each module is completed, the whole system needs to be tested (i.e., all modules functioning together). Even though each module may work satisfactorily, when they are all put together there may be data clashes or incompatibility, memory issues, etc.

All of this may lead to a need to improve the input and output methods, file/database structures, validation and verification methods, etc., and then test everything fully again. It is a very time-consuming process but it has to be as perfect as possible before the system goes live.

Testing will use many different types of test data, which will fall into one of

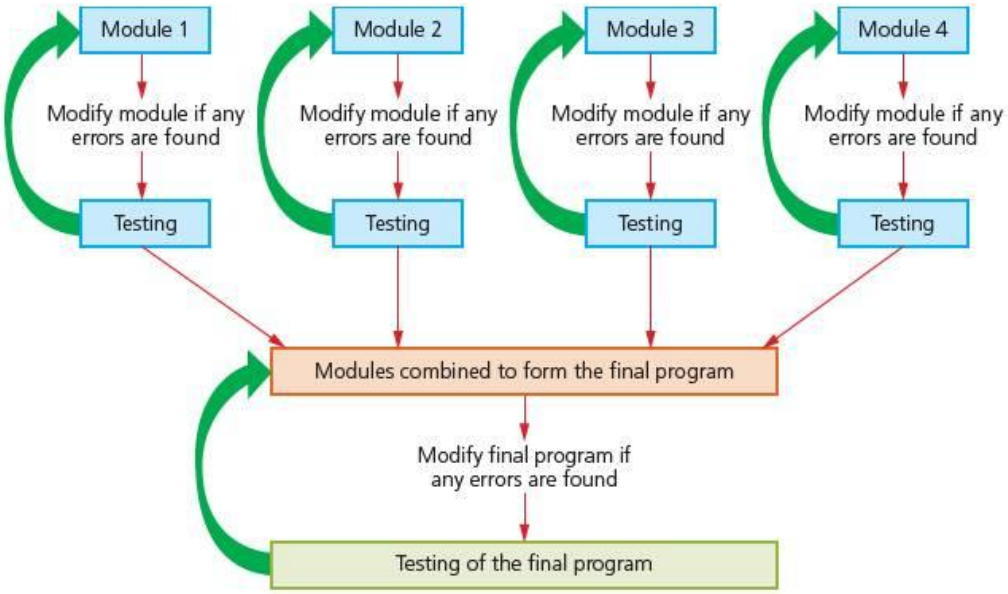


Figure 7.10 Module testing

four categories:

- normal
- abnormal
- extreme
- live.

But we are only going to consider the first three types at this stage.

Let us suppose that one of the fields in a database is the date, which must be in the form dd/mm/yyyy (and also has to be numeric):

- **normal**: this is data that is acceptable/reasonable and has an expected (known) outcome; for example, the month can be *any* whole number in the range 1 to 12
- **extreme**: this is data at the **limits** of acceptability; for example, the extreme values of month can be either 1 **or** 12
- **abnormal**: this is data **outside the limits** of acceptability, or the wrong type of data, and should be rejected or cause an error message; for example, all the following values are not allowed as inputs for the month:
  - negative numbers (e.g., –1, –15, etc.)
  - any value greater than 12 (e.g., 32, 45, etc.)
  - letters or other non-numeric data (e.g., July, etc.)
  - non-integer values (e.g., 3.5, 10.75, etc.).

Once a system has been fully tested, it is then tested with **live data** – this is data

Exercise 7c

Use the example of a date in the format dd/mm/yyyy when answering these three questions.

1 Consider the following eight pieces of data and decide whether each data item is normal, extreme or abnormal (tick the appropriate box) for:
   a day (dd)
   b month (mm)
   c year (yyyy).

Data item	Normal	Extreme	Abnormal
15			
12			
7			
1.6			
0			
1			
March			
10			

2 Describe what validation routines could be used to check the date if it was input on the screen as follows:

Day: ☐

Month: ☐

Year: ☐

Describe how it would be possible to avoid errors altogether when inputting the date in the form shown above.

3 Write test data for the following fields in a database (the data should try to cover all possible types of data). The database will store the following information:

- name of resort
- average daily temperature
- number of hours of sunshine per day.

Describe the validation routines that should be written into the database interface to check the above inputs.

with known outcomes. Live data is entered into the new system and the results compared with those produced from the existing system. Further modifications to the software may be needed following this testing procedure.

An example of a results comparison table is shown in Table 7.4.

Table 7.4 Live data comparison table

Live data	Expected result	Actual result	Any actions
January	error message	data was accepted	validation routines on month element need to be altered
0	message output: 'a zero value is not allowed'	computer software crashed	software needs an error trap, such as: IF INPUT = 0 THEN OUTPUT 'no zeros allowed'

7.4 Implementation

Once the system is fully tested, the next stage is to fully implement it. Some of the stages in this process are shown in Figure 7.11.

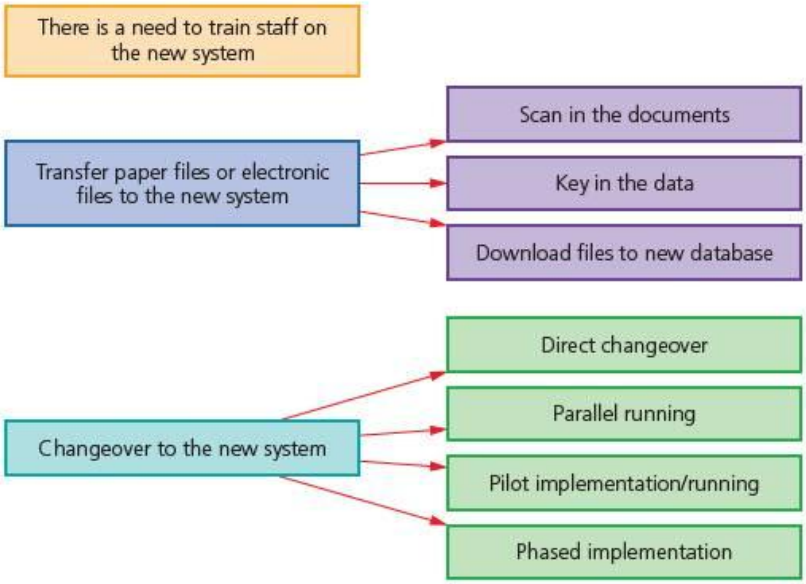


Figure 7.11 The implementation stage

We will now consider **changeover** to the new system in more depth. As indicated above, there are four common methods used for changing over from the old system to the new system. Each one has advantages and disadvantages that need to be weighed up before the most appropriate method is chosen for a particular application.

Table 7.5 Methods of changeover

Implementation method	Design of implementation method	Advantages and disadvantages of the method
Direct	With this method the old system is stopped overnight and the new system introduced immediately	• this method can be disastrous if the new system fails since the old system is no longer available • the benefits are immediate • costs are reduced (since only one system used there is no need to pay for two sets of staff) • less likelihood of a malfunction since the new system will have been fully tested
Parallel	With this method, the old and new systems are run side by side for a time before the new system takes over altogether	• if this new system fails, the old system is still available as a backup • it is possible to gradually train staff • it is more expensive than *direct* since extra staff are needed to run both systems together • it's also more time consuming than *direct* since data needs to be entered into two systems
Pilot	With this method, the new system is introduced into one branch or office of the company and its performance assessed before being introduced elsewhere in the company	• if the new system fails, only one part is affected; the remainder is unaffected • it is possible to train staff in one area only, which is much faster and less costly than *parallel* • the costs are also less than *parallel* since only one part of the system is being used in the pilot warehouse
Phased	With this method, only part of the new system is introduced and, only when it proves to work satisfactorily, is the next part introduced, and so on, until the old system is fully replaced	• if the latest part fails, it is only necessary to go back in the system to the point of failure; hence failure isn't disastrous • more expensive than *direct* since it is necessary to evaluate each phase before moving to the next stage • very time consuming since each part needs to be fully evaluated before making any further changes to the system • it is possible to ensure the system works properly before expanding

Table 7.6 compares the costs, input requirements and risk of failure for all four changeover methods.

Table 7.6 Impact of changeover methods

Changeover method	Relative costs of each method	Input needed by the user	Input needed by systems team	Impact of failure of method
Parallel	High	High	Low	Low
Pilot	Medium	Low	Medium	Low
Phased	Medium	Medium	Medium	Medium
Direct	Low	Medium	Low*	High

*Low if successful, otherwise very high because of amount of input needed.

7.5 Documentation

Once the new system is fully developed, a considerable amount of documentation also needs to be produced for:

1. the end-user
2. people who may need to modify or develop the system further at some later stage.

There is some overlap between the two types of documentation, but the basic requirements are shown below.

7.5.1 User documentation

User documentation is designed to help users to learn how to use the software or system. This can consist of any of the following:

- how to load/install/run the software
- how to save files
- how to do a search
- how to sort data
- how to do print outs
- how to add, delete or amend records
- the purpose of the system/program/software package
- limitations of the system
- screen layouts (input format)
- print layouts (output format)
- hardware requirements
- software requirements
- sample runs (with results and actual test data used)
- error handling/meaning of errors
- troubleshooting guide/help lines/FAQs
- how to log in/log out
- tutorials
- error messages/meaning of error messages
- glossary of terms.

7.5.2 Technical documentation

Technical documentation is designed to help programmers/analysts to make improvements to the system or to repair/maintain the system. This can consist of any of the following:

- program listing/coding
- programming language used
- program flowcharts/algorithms
- systems flowcharts
- purpose of the system/program/software
- limitations of the system
- input formats
- hardware requirements
- software requirements
- minimum memory requirements
- known 'bugs' in the system
- list of variables used (and their meaning/description)
- file structures
- sample runs (with results and actual test data used)
- output formats
- validation rules
- meaning of error messages.

7.6 Evaluation

Once a system is up and running it is necessary to do some **evaluation** and carry out any maintenance if necessary. The following is a list of some of the things considered when evaluating how well the new system has worked; this can ultimately lead to a redesign of part of the system if there is strong evidence to suggest that changes need be made (refer back to Figure 7.1 in the introduction):

- compare the final solution with the original task
- identify any limitations of the system
- identify any necessary improvements that need to be made
- evaluate the user's responses to using the new system
- compare test results from the new system with results from the old system
- compare performance of the new system with performance of the old system
- observe users performing set tasks (compare old with new)
- measure the time taken to complete tasks (compare old with new)
- interview users to gather responses about how well the new system works
- give out questionnaires to gather responses about the ease of use of the new system.

Some results from the evaluation may lead to two things happening:

- update of hardware because:
  - of feedback from end-users
  - new hardware comes on the market, necessitating change
  - changes within the company require new devices to be added or updated
- update of software because:
  - of feedback from end-users
  - changes to the company structure or how the company works that may require modifications to the software
  - changes in legislation that may require modifications to the software.

8 Safety and security

In this chapter you will learn about:

- safety and security when using computers
- data security
- firewalls
- security protocols (SSL and TLS)
- encryption
- authentication.

This chapter covers safety and security issues when using computers in the office or at home. As the use of computers continues to expand, the health risks and security risks continue to increase. Many of these risks are associated with the internet which, by its very nature, poses a great risk to younger people unless they are vigilant at all times. But large businesses are also at risk from hackers, pharming attacks and viruses, for example. Many of the precautions people and business can take are common sense but, equally, it also requires additional knowledge to know how to protect yourself from these external attacks, which can come from anywhere in the world.

8.1 Physical security

The use of computers in the home and business world has increased dramatically over the last few years. This increase brings its own physical dangers, which can cause harm to users unless they take some very sensible precautions.

8.1.1 Health aspects

Health and safety regulations advise that all computer systems have at least tiltable and anti-glare screens, adjustable chairs and foot supports, suitable lighting and uncluttered work stations, and recommend frequent breaks and frequent eye tests.

Table 8.1 lists a number of health risks as well as giving some idea of how each risk can be removed or minimised.

Table 8.1 Health risks

Health risk	Ways of eliminating or minimising risk
Back and neck problems/strain caused by sitting in front of a computer screen for long periods in the same position)	• use fully adjustable chairs to give the correct posture • use foot rests to reduce posture problems • use screens than can be tilted to ensure the neck is at the correct angle
Repetitive strain injury (RSI) – damage to fingers and wrists caused by continuous use of a keyboard or repetitive clicking of mouse buttons, for example	• ensure correct posture is maintained (i.e., correct angle of arms to the keyboard and mouse, for example) • make proper use of a wrist rest when using a mouse or a keyboard • take regular breaks (and do some exercise) • make use of ergonomic keyboards • use voice-activated software if the user is prone to problems when using a mouse and keyboard
Eyestrain caused by staring at a computer screen too long or having incorrect lighting in the room	• ensure that there is no screen flicker as this can lead to eye problems • change to LCD screens where flicker is less of a problem than with CRT screens • take regular breaks (and try focusing on a point that is some distance away) • make use of anti-glare screens if lighting in the room is incorrect; or use window blinds to reduce sunlight reflecting from the screen • users should have their eyes tested on a regular basis (middle vision glasses should be prescribed if the user has a persistent problem such as eye strain, dry eyes, headaches, etc.)

⇨ continued...

Headaches caused by incorrect lighting, screen reflections, flickering screens, etc.	• use an anti-glare screen or use window blinds to cut out reflections (incorrect lighting can cause squinting and lead to headaches) • take regular breaks (and do some exercise) • have your eyes tested regularly and use middle vision glasses if necessary
Ozone irritation caused by laser printers in an office area (dry skin, respiratory problems, etc.)	• proper ventilation should exist to remove the ozone gas as quickly as possible • laser printers should be housed in a designated printer room • change to other types of printer if necessary (e.g., inkjet printers)

8.1.2 Safety aspects

Safety is a different issue to health; health is more generally how to stop people becoming ill or being affected by daily contact with computers. Safety is more concerned with dangers that could lead to serious injury or even loss of life. Some of the more common examples of **safety risks**, together with possible solutions, are listed in Table 8.2.

Table 8.2 Safety risks

Safety risk	Ways of eliminating or minimising risk
Electrocution	• use an RCB (residual current breaker) • check insulation on wires regularly • don't allow drinks near computers • check equipment on a regular basis
Trailing wires (trip hazard)	• use cable ducts to make the wires safe • cover wires and/or have them neatly tucked away (under desks, etc.) • use wireless connections wherever possible, thus eliminating cables altogether
Heavy equipment falling and causing injury	• use strong desks and tables to support heavy hardware • use large desks and tables so that hardware isn't too close to the edge where it can fall off
Fire risk	• have a fully tested CO_2/dry fire extinguisher nearby (not water extinguishers) • don't cover equipment vents (causing equipment to overheat) • make sure that the electrics used in the hardware is fully maintained (i.e. portable appliance testing) • ensure good ventilation in the room (again to stop overheating of hardware) • don't overload sockets with too many items • change to low-voltage hardware wherever possible (e.g., replace CRT monitors with LCD monitors)

In spite of all the above ways of eliminating or reducing the health and safety risks, the individual still has an important role to play. In the home, the user needs to have a good health and safety strategy, and to carry out the following checks on a regular basis:

- check the state of the wires/cables and plugs (check whether any wires/cables are damaged, make sure there are no lose wires in the plugs and make sure the plug isn't broken or cracked)
- make sure that drinks (such as tea or coffee) are well away from the computer
- fix wires along walls and behind desks wherever possible to remove the risk of wires coming into contact with people
- don't cover computers with paper or fabric (e.g., towels or sheets) since these can either block ventilation holes (causing computers to overheat) or these materials could catch fire
- don't plug too many devices into an electric outlet socket – overloading a socket can cause a fire

- make sure you exercise every hour or so to prevent the health risks outlined Table 8.1 from becoming a real issue
- carry out an 'ergonomic assessment' on your work station (there are numerous online questionnaires that will enable you to check whether your work station is set up properly for your own health and safety); it may require you to buy new chairs or computer hardware to minimise the impact of sitting in front of screens or typing for long periods at a time.

8.2 E-safety

First of all, what is the definition of **e-safety**? It refers to safety when using the internet, i.e. keeping personal data safe and applies to any of the following devices:

- mobile phone
- computer or tablet
- games console
- wireless technology.

Personal data refers to any data concerning a living person who can be identified either from the data itself or from the data in conjunction with other information (for example, 'Peter Smith has blue hair and lives at 40 Green Street' would very clearly identify this individual).

Examples of personal data include:

- name
- address
- date of birth
- medical history
- banking details.

Some personal data is often referred to as **sensitive personal data** and includes:

- ethnic origin
- political views
- religion
- sexual orientation
- criminal activity.

Exercise 8a

Do some research and find out why it is important that personal data is kept confidential. Present your notes as an article to discuss with the rest of the class.

E-safety also refers to the benefits, risks and responsibilities when using ICT. The following list is by no means exhaustive but gives some idea of the e-safety issues that can be encountered by users of ICT hardware:

- don't give out any personal information to people who are unknown to you; this is especially true online where it isn't possible to physically meet people so that their motives can be fully assessed. Remember that anyone can say anything they want online and it is very difficult to determine whether they are genuine or not
- don't send people photos of yourself – either online or via a mobile phone – unless the person is known to you (it is very easy for somebody to pass

these photos on or even pretend to be you for a number of reasons); this is a particularly large risk on social networking sites
- always maintain your **privacy settings** on whatever device is being used online or during communications. Privacy settings allow the user to control which cookies are stored on their computer or they enable the user to decide who can view certain information about them on, for example, a social networking site
- when accessing the internet make sure the websites being visited can be trusted (two common ways of checking this is to look for https or the padlock sign ); when using search engines, always make sure the device settings are set to 'safe search' and the highest possible level of security is used
- only use websites recommended by teachers and only use a learner-friendly search engine
- only open emails from known sources. It is always a good idea to make sure your internet service provider (ISP) has an effective email filtering feature to ensure unknown emails are placed in the **spam** box
- only email people you know. Think carefully before opening any email and never include the school's name or photos of a student wearing a school uniform in any email
- it is extremely important to be vigilant when using social networking sites, instant messaging or chat rooms:
  - block or report anybody who acts suspiciously or who uses inappropriate language
  - be very careful with the language used in chat rooms
  - always use a nickname and *never* your real name
  - keep private and personal data secret
  - don't enter private chat rooms – stay public (the danger signs in a private chat are: somebody sounds too good to be true, they ask you to go to instant messaging and then to emails, they request your telephone number and then finally suggest that you meet)
  - never arrange to meet anyone for the first time on your own
  - always tell an adult first and meet the person in a public place
  - avoid the misuse of images
  - always use appropriate language
  - always respect people's confidentiality.

It is also important to be careful when using online gaming since this carries its own risks. Many users think that all players are like-minded and, thus, there are no real risks associated with this type of communication. Some of the known risks reported over the years include:

- violence in the game itself, which can lead to violent behaviour in reality
- predators (people who prey on others who they see as vulnerable)
- cyber bullying (the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature)
- use of webcams (the risks here are obvious)
- voice-masking technology (to disguise a voice so you can't tell their sex or age, or even their accent)
- it is often overlooked that online games are also a source of cyber attacks on a user's computer or mobile phone – viruses, phishing or spyware are well-reported examples of problems associated with certain online gaming.

Exercise 8b

Evaluate your own use of email and social media/ networking sites. Which of these e-safety strategies do you use?

Exercise 8c

Find out what safety measures should be taken when playing games on the internet. Write an article on these safety measures and also include ways to minimise or remove these risks.

The above list is by no means exhaustive but gives some idea of the risks associated with using computers and tablets online. It also indicates that gaming and the use of mobile phones carry equal risks. Basically, any device that allows communication (either through the internet, via phone networks or even via wireless communications) has a number of associated risks. As long as users take simple precautions, the risks are considerably minimised and ICT can be used to its full.

8.3 Security of data

There are a number of **security risks** associated with any electronic device that connects to a network (internet or mobile phone networks being the most common). This section covers the following risks:

- hacking
- phishing
- smishing
- vishing
- pharming
- spyware
- viruses
- spam
- moderated and unmoderated forums
- cookies.

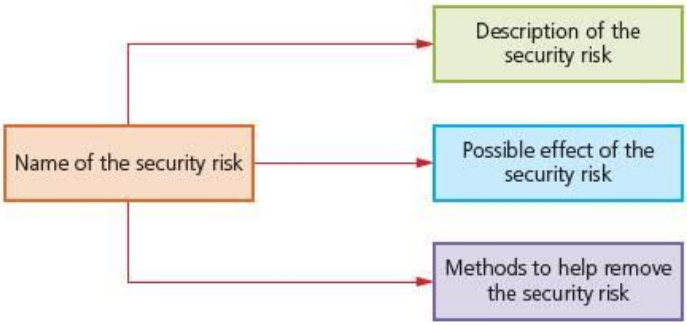


Figure 8.1 Security risks

Each security risk, together with its description, possible effects and how to minimise it, will be set out as shown in Figure 8.1.

8.3.1 Hacking

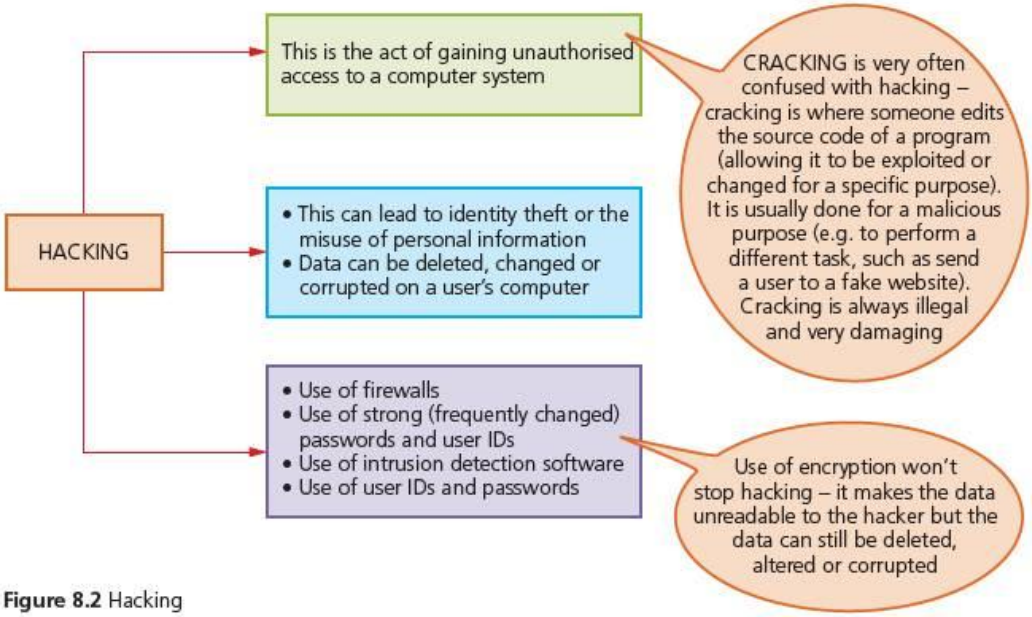


Figure 8.2 Hacking

8.3.2 Phishing

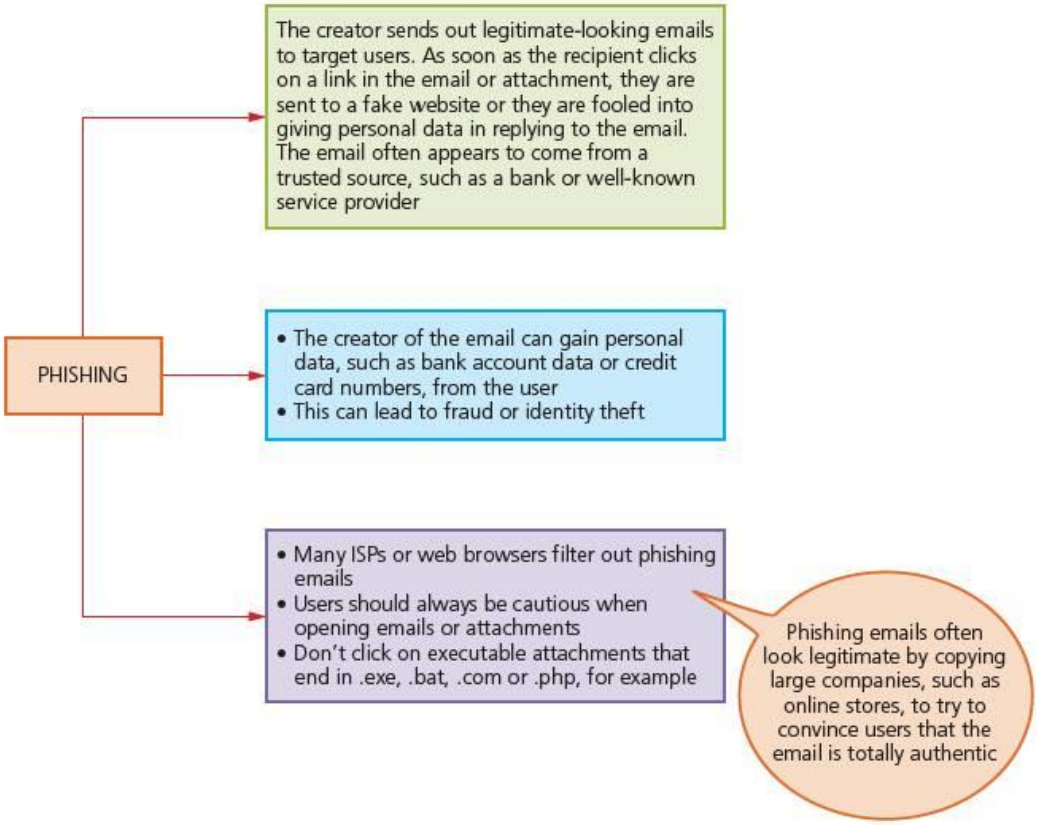


Figure 8.3 Phishing

Malicious use refers to, for example, deletion, fraud, identity theft and selling on personal data. A good example of a phishing attack is when a user is sent an email saying they have ordered an item from an online store. They will be asked to click on a link to see the order details. The link takes the user to a page that shows a product code from a well-known company. A message such as: 'if this order wasn't made by you, please fill out the following form to cancel your order in the next 24 hours' is given. The form will ask for details such as credit card number, user's address and so on. Some of the key clues are that links, such as how to 'contact us', don't work.

Smishing – short for SMS phishing – uses the SMS system of mobile phones to send out fake text messages. It is very similar to phishing as described earlier. These scams often contain a URL or telephone number embedded in the text message. The recipient will be asked to log on to the website or make a telephone call. If they do, they will be asked to supply personal details such as credit/debit card numbers or passwords. As with phishing attacks, the text message will appear to come from a legitimate source and will make a claim, for example, that they have won a prize or that they need to contact their bank urgently. Most people believe that only computers are liable to security threats; mobile phones aren't at risk. This makes smishing a particularly dangerous security threat to many people.

Vishing (voice mail phishing) is another variation of phishing. This uses a voice mail message to trick the user into calling the telephone number contained in the message. As with all phishing attacks, the user will be asked to supply personal data thinking they are talking to a legitimate company.

8.3.3 Pharming

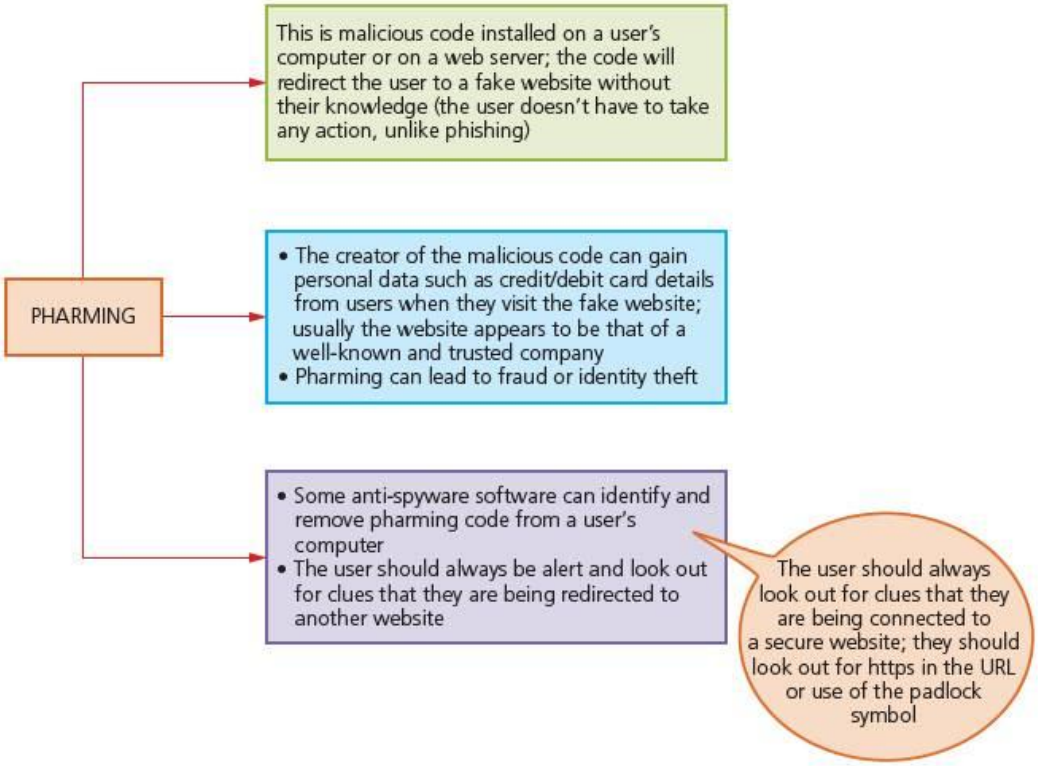


Figure 8.4 Pharming

8.3.4 Spyware and key-logging software

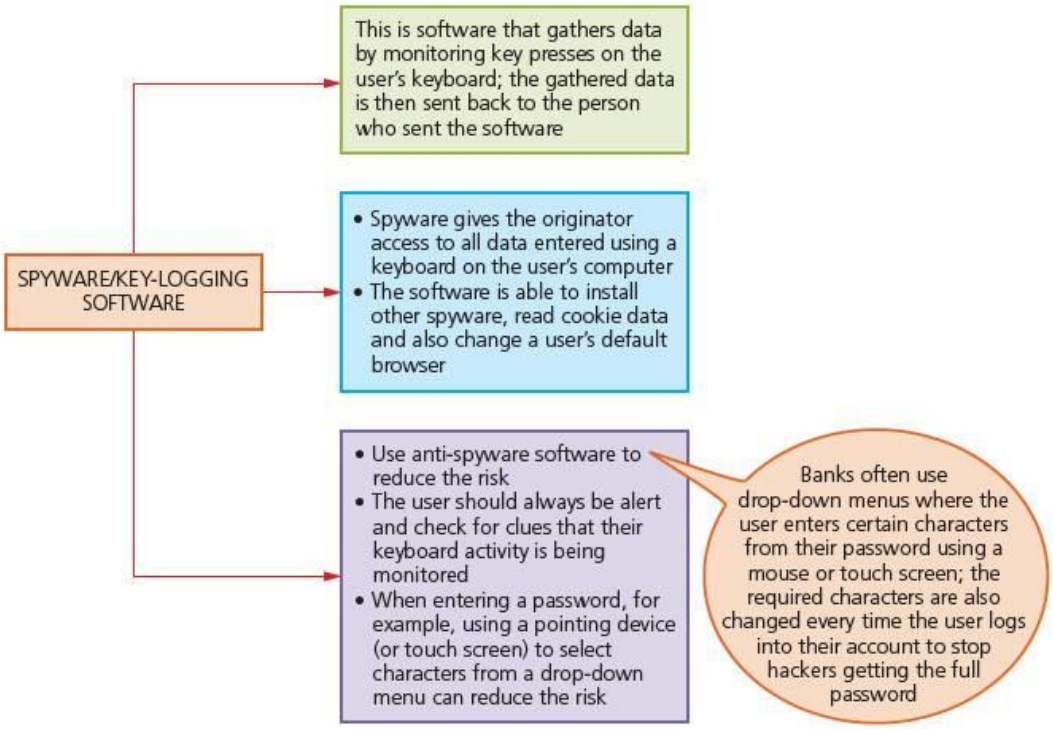


Figure 8.5 Spyware and key-logging software

8.3.5 Viruses

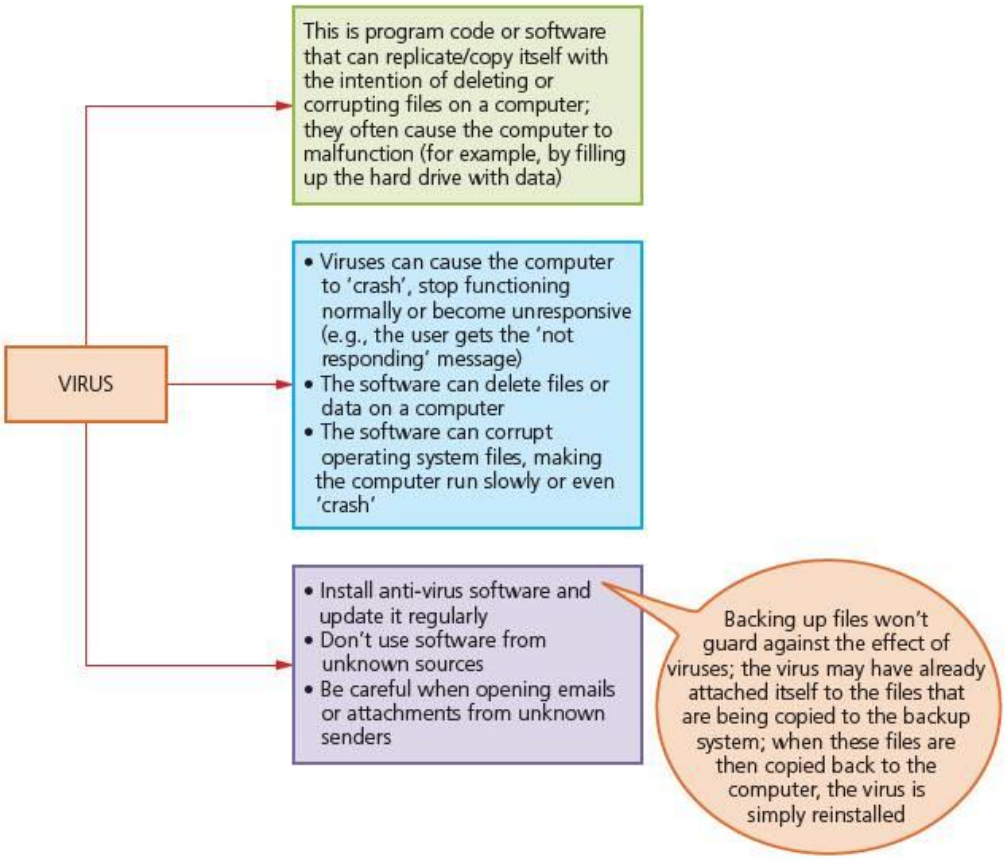


Figure 8.6 Viruses

8.3.6 Spam

Spam, often referred to as junk email, is usually sent out to a recipient who is on a mailing list or mailing group. Spammers obtain these email addresses from chat rooms, websites, newsgroups and even certain viruses that have been set up to harvest a user's contacts list. While spam is rarely a security risk, it can lead to **denial of services**, for example, by 'clogging up' the bandwidth on the internet. Denial of services is basically an attack on a network that is designed to slow the network down by flooding it with useless traffic. However, spam can be linked to phishing attacks or even the spread of computer viruses, so it should be treated with some caution.

Many ISPs filter out spam or junk mail. However, some of the more overactive ISPs can filter out 'wanted' emails that come from new sources.

Spam prevention techniques

- To obtain the maximum protection possible when using the 'junk email filter' set the protection level to high or to safe lists only. Make sure the junk mail filter is kept up to date.
- Block images in HTML messages that spammers use as web beacons (a web beacon can be a graphic image, linked to an external web server, that is placed in an HTML-formatted message and can be used to verify that your email address is valid when the message is opened and images downloaded).

- Look out for check boxes that are already selected when items are bought online; companies sometimes add a check box (which is already selected) to indicate that you have agreed to sell or give your email address to third party users; make sure that this check box is 'unticked' so that your email address can't be shared.
- Do not sign up to commercial mailing lists.
- Do not reply to an email or unsubscribe from a mailing list that you did not explicitly sign up to in the first place.

8.3.7 Moderated and unmoderated forums

A **moderated forum** refers to an online discussion forum in which all the posts are checked by an administrator before they are allowed to be posted. Many users prefer this type of forum, compared to an unmoderated one, as the moderator can not only prevent spam, but can also filter out any posts that are inappropriate, rude or offensive, or even those that wander off the main topic.

The internet is essentially an **unmoderated forum**. No one 'owns' the internet, and it is essentially not policed (this is discussed in more depth in Chapter 9). The only real safeguards are a voluntary cooperation between the users and the network operators. However, most social forums or networking groups on the internet have a set of rules or protocols that members are requested to follow or they will be deleted.

8.3.8 Cookies

Cookies are small files or code that are stored on a user's computer. They are sent by a web server to a user's computer. Each cookie is effectively a small look-up table containing pairs of (key, data) values; for example (surname, Jones) and (music, rock). Once the cookie has been read by the code on the web server or user's computer, the data can be retrieved and used to customise the web page for each individual. These are often referred to as user preferences. For example, when a user buys a book online, the cookies remember the type of book the user chose and the web page will then show a message such as: 'Customers who bought *Cambridge IGCSE ICT* also bought *Cambridge IGCSE Computer Science*'.

The data gathered by cookies forms an **anonymous user profile** and doesn't contain personal data such as passwords or credit/debit card numbers. Cookies are a very efficient way of carrying data from one website session to another, or even between sessions on related websites. They remove the need to store massive amounts of data on the web server itself. Storing the data on the web server without using cookies would also make it very difficult to retrieve a user's data without requiring the user to login every time they visit the website.

Use of secure servers is always advised. A secure web server is one that supports any of the major security protocols, such as SSL/TLS, that encrypt and decrypt messages to protect them against third party eavesdropping. Making purchases from a secure web server ensures that a user's payment or personal information can be translated into a secret code that's difficult to break.

8.4 Additional security of data online

This section discusses additional ways of keeping data secure when accessing external systems, such as the internet. We will consider:

- firewalls
- security protocols
- encryption
- authentication.

8.4.1 Firewalls

A **firewall** can be either software or hardware. It sits between the user's computer and an external network (for example, the internet) and filters information coming in and out of the user's computer.

Figure 8.7 Firewall

The following list shows a number of the tasks carried out by a firewall:

- to examine the 'traffic' between a user's computer (or internal network) and a public network (for example, the internet)
- checks whether incoming or outgoing data meets a given set of criteria
- if the data fails the criteria, the firewall will block the traffic and give the user (or network manager) a warning that there may be a security issue
- the firewall can be used to log all incoming and outgoing traffic to allow later interrogation by the user (or network manager)
- criteria can be set so that the firewall prevents access to certain undesirable sites; the firewall can keep a list of all undesirable IP addresses
- it is possible for firewalls to help prevent viruses or hackers entering the user's computer network
- it is also possible for firewalls to help prevent hackers gaining access to the user's computer or network. This can be done by blocking IP addresses, but it should be pointed out that hackers can still have access to a computer or network if they are using an **allowed** computer
- the user is warned if some software on their system is trying to access an external data source (for example, an automatic software upgrade); the user is given the option of allowing it to go ahead or request that such access is denied.

The firewall can be a hardware interface that is located somewhere between the computer and the internet connection, in which case it is often referred to as a **gateway**. Alternatively, the firewall can be software installed on a computer; in some cases this is part of the operating system.

However, there are certain circumstances where the firewall can't prevent potential harmful traffic:

- it cannot prevent individuals, on internal networks, using their own modems to bypass the firewall
- employee misconduct or carelessness cannot be controlled by firewalls (for example, control of passwords or user accounts)
- users on stand-alone computers can choose to disable the firewall, leaving their computer open to harmful traffic from the internet.

All of these issues require management control (or personal control on a single computer) to ensure that the firewall is allowed to do its job effectively.

8.4.2 Security protocols

We will now consider two forms of security protocols – sets of rules used by computers to communicate with each other across a network – when using the internet:

- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS).

Secure Sockets Layer (SSL) is a type of protocol that allows data to be sent and received securely over the internet.

When a user logs on to a website, SSL encrypts the data – only the user's computer and the web server are able to make sense of what is being transmitted. A user will know if SSL is being applied when they see https (as part of the website address) or the small padlock in the status bar at the top of the screen. Figure 8.8 shows what happens when a user wants to access a secure website and receive and send data to it.

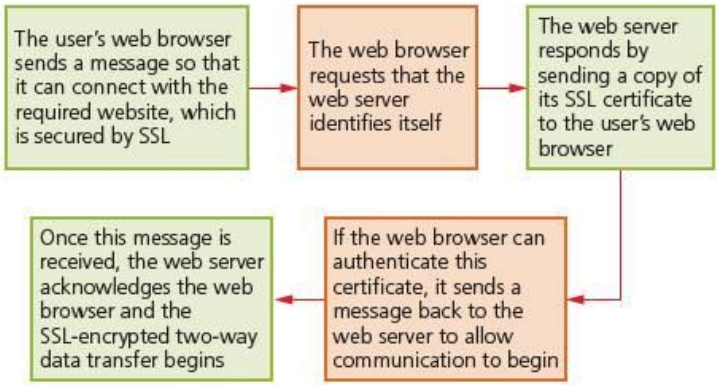


Figure 8.8 Communicating across a network using SSL

Note: SSL certificates are small data files that digitally bind an encryption key to an organisation's details. When installed on a web server, it shows as the green padlock and the https protocol and ensures secure connections from a web server to a web browser.

Transport Layer Security (TLS) is similar to SSL but is a more recent security system. TLS is a form of protocol that ensures the security and privacy of data between devices and users when communicating over the internet. It is essentially designed to provide encryption, authentication and data integrity (data integrity is maintaining the accuracy and the consistency of data) in a more effective way than its predecessor, SSL.

When a website and a user communicate over the internet, TLS is designed to prevent a third party hacking into this communication and causing problems with data security.

TLS is formed of two layers:

- **Record Protocol**: this part of the communication can be used with or without encryption (it contains the data being transferred over the internet).
- **Handshake Protocol**: this permits the website and the user to authenticate each other and to make use of encryption algorithms (a secure session between user and website is established).

Only the most recent web browsers support both SSL and TLS, which is why the older SSL is still used in many cases. But what are the main differences between SSL and TLS, since they both effectively do the same thing?

- it is possible to extend TLS by adding new authentication methods
- TLS can make use of **session caching**, which improves the overall performance compared to SSL (see the note below to explain this term)
- TLS separates the handshaking process from the record protocol (layer), which holds all the data.

Session caching

When opening a TLS session, it requires a lot of computer time (due mainly to the complex encryption keys being used). The use of session caching can avoid the need to utilise so much computer time for each connection. TLS can either establish a new session or attempt to resume an existing session; using the latter can boost system performance considerably.

Note: a cache is a collection of processed data that is kept on hand and reused in order to avoid costly repeated database queries.

8.4.3 Encryption

Encryption is used primarily to protect data in case it has been hacked or accessed illegally. While encryption won't prevent hacking, it makes the data meaningless unless the recipient has the necessary decryption tools described below.

Encryption uses a secret key that has the capability of altering the characters in a message. If this key is applied to a message, its content is changed, which then makes it unreadable unless the recipient also has the same secret key. When this secret key is applied to the encrypted message, it can be read.

The key used to encrypt (or encode) the message is known as the **encryption key**; the key used to decrypt (or decipher) the message is known as the **decryption key**. When a message undergoes encryption it becomes **cypher script**; the original message is known as **plain text**. Figure 8.9 shows how these are linked together.

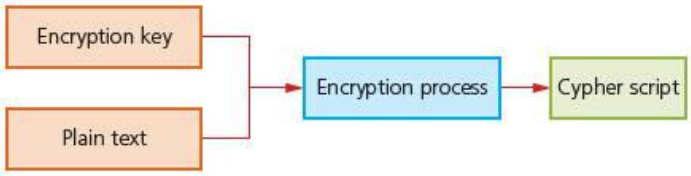


Figure 8.9 Encryption

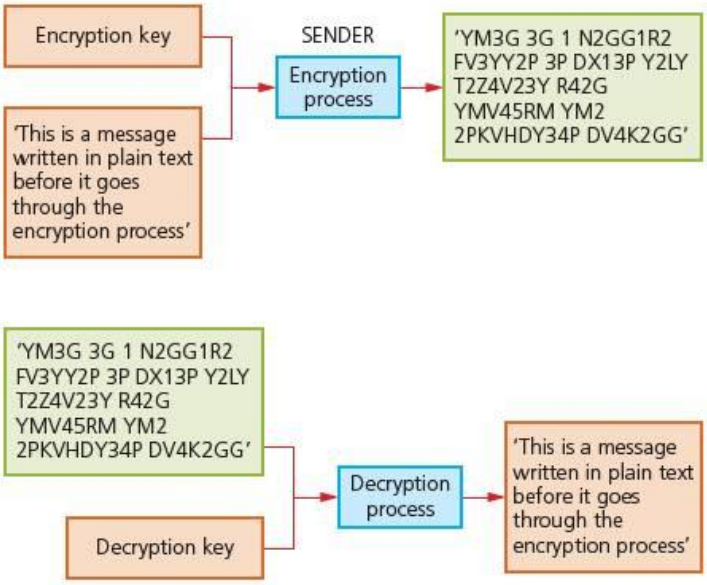


Figure 8.10 Example of the encryption and decryption process

8.4.4 Authentication

Authentication is used to verify that data comes from a secure and trusted source. It works with **encryption** to strengthen internet security. In this section we will consider digital certificates, passwords and biometrics in their authentication roles.

Digital certificates

A **digital certificate** is a pair of files stored on a user's computer – these are used in the security of data sent over the internet. Each pair of files is divided into:

- a public key (which is known by anyone)
- a private key (known to the computer user only).

For example, when sending an email, the message is made more secure by attaching a digital certificate. When the message is received, the recipient can verify that it comes from a known or trusted source by viewing the public key information (this is usually part of the email attachment). This is an added level of security to protect the recipient from harmful emails. The digital certificate is made up of six parts:

Figure 8.11 Digital IDs

- the sender's email address
- the name of the digital certificate owner
- a serial number
- expiry date (the date range during which the certificate is valid)
- public key (used for encrypting messages and for digital signatures)
- digital signature of certificate authority (CA) – an example of this is VeriSign.

Operating systems and web browsers maintain lists of trusted CAs (see Figure 8.11 for an example).

Passwords

When logging on to a system (for example, a bank website), a user will be asked to type in their **password** – this should be a combination of letters and numbers that would be difficult for somebody else to guess. Strong passwords should contain upper case and lower case characters, as well as numbers and other keyboard symbols, for example: Rn5K;2mL/8.

When the password is typed in, it often shows on the screen as ******** so nobody overlooking can see what the user has typed in. If the user's password doesn't match up with the user ID then access will be denied. Many systems ask for the password to be typed in twice as a verification check (check on input errors). To help protect the system, users are only allowed to type in their password a certain number of times – usually three times is the maximum number of tries allowed – before the system locks the user out. After that, the user will be unable to log on until the system administrator has reset their password.

For example, if a user forgets their password when using the internet, they can request that the password is sent to their email address. The password is never shown on the computer screen for reasons of security.

Passwords should be changed on a regular basis in case they become known to another user or even a hacker. In particular, it is important to prevent other people gaining access to your password by way of spyware or viruses – many methods to guard against this have been discussed earlier in this chapter.

It is often necessary to use a user ID or log in ID as well as a password. This gives an additional security level since the user ID and password must match up to allow a user to gain access to, for example, a bank website.

Biometrics

Biometrics relies on certain unique characteristics of human beings; examples include:

- fingerprint scans
- signature recognition
- retina scans
- iris recognition
- face recognition
- voice recognition.

Biometrics is used in a number of applications as a security device. For example, some of the latest mobile phones use fingerprint matching before they can be operated; some pharmaceutical companies use face recognition or retina scans to allow entry to secure areas. We will now consider two of these biometric techniques in a little more detail.

Fingerprint scans

Images of fingerprints are compared against previously scanned fingerprints stored in a database; if they match then access is allowed. The system compares patterns of 'ridges' and 'valleys', which are fairly unique (accuracy is about one in 500).

An example of its use would be as a security method for entering a building. Fingerprint scanning techniques have the following advantages in this application:

- everybody's fingerprints are unique, therefore this technique would improve security since it would be difficult to replicate a person's fingerprints
- other security devices (such as magnetic cards) can be lost or even stolen, which makes them less effective
- it would be impossible to 'sign in' for somebody else since the fingerprints would match up to one person only on the database
- fingerprints can't be misplaced; a person always has them!

What are the disadvantages in this application?

- relatively expensive to install and set up
- if a person's fingers are damaged through an injury, this can have an effect on the scanning accuracy
- some people may regard it as an infringement of civil liberties.

Retina scans

Retina scans use infrared light to scan the unique pattern of blood vessels in the retina (at the back of the eye). It is a rather unpleasant technique, requiring a person to sit totally still for 10 to 15 seconds while the scan takes place. It is very secure as nobody has yet found a way to duplicate blood vessels patterns (the accuracy is about one in ten million).

Table 8.3 Comparison of the six common biometric techniques

Biometric technique	Comparative accuracy	Comparative cost	Devices needed	Social acceptability	What can interfere with the procedure
Fingerprint scans	high accuracy	medium	scanner	medium	damaged fingers (e.g., cuts)
Signature recognition	low accuracy	medium	an optical pen	high	signatures can change with time
Retina scans	high accuracy	high	digital camera	low	irritation of the eye
Iris recognition	high accuracy	high	digital camera	low	wearing of glasses
Face recognition	medium–low accuracy	medium	digital camera	high	facial hair or glasses
Voice recognition	medium accuracy	medium	microphone	high	background noise or person has a cold

Table 8.4 Comparison of the advantages and disadvantages of the six common biometric techniques

Biometric technique	Advantages	Disadvantages
Fingerprint scans	• one of the most developed biometric techniques • very high accuracy • very easy to use • relatively small storage requirements for the biometric data created	• for some people it is very intrusive, since it is still related to criminal identification • it can make mistakes if the skin is damaged (e.g., cuts)
Signature recognition	• non-intrusive • requires very little time to verify (about five seconds) • relatively low-cost technology	• if individuals do not sign their names in a consistent manner there may be problems with signature verification • high error rate (one in 50)
Retina scans	• very high accuracy • there is no known way to replicate a person's retina	• it is very intrusive • it can be relatively slow to verify retina scan with stored scans • very expensive to install and set up
Iris recognition	• very high accuracy • verification time is generally less than five seconds	• very intrusive • uses a lot of memory for the data to be stored • very expensive to install and set up
Face recognition	• non-intrusive method • relatively inexpensive technology	• it is affected by changes in lighting, the person's hair, their age, and if the person is wearing glasses
Voice recognition	• non-intrusive method • verification takes less than five seconds • relatively inexpensive technology	• a person's voice can be recorded easily and used for unauthorised access • low accuracy • an illness, such as a cold, can change a person's voice, making absolute identification difficult or impossible

Exercise 8d

Find out which applications use each of the biometric techniques described in this section. Consider all the advantages and disadvantages of each method and make conclusions about its suitability for the applications you found.

Online credit fraud

In spite of all the security systems described above, online credit card fraud is still too common. It basically happens for the following reasons:

- hackers gaining access to a user's computer through the use of spyware, phishing or pharming; any of these methods can trick a user who is not particularly IT literate; the user can be tricked into giving personal and financial details that enable the hacker to gain full access to a user's account; this can lead to unauthorised purchases or even removal of money from an account if it remains undetected for a few days
- the breaking of passwords through a number of techniques is an all-too-familiar risk; if passwords are weak or no encryption is used then it is a relatively easy task to break these passwords and allow illegal access to bank and credit card accounts
- it is always a good idea to type in a web address or URL rather than 'copy and paste it' from an email or other website. Sometimes the web address/URL is altered very slightly in the email and the user ends up visiting a fake website. Once they visit the fake website it is possible that they will give personal and financial details to a fraudster without the user's knowledge – by physically typing in the web address the user will ensure they get it right and avoid such risks
- if the user is using wireless technology, it is very important for internet access to be password controlled since it is relatively easy to tap in to wireless networks without password protection

- if a user logs in to an account or website in a public place (such as an airport using the available Wi-Fi 'hotspots') it is necessary to be very vigilant; there is always a risk that somebody is monitoring internet usage in the area and will try to tap in to the data that is going to and from any computer using this wireless link
- even large organisations can be subject to cybercrime; in recent years, the cloud and some large retail companies have been the targets for hackers, which leaves customers very vulnerable.

There are a number of simple precautions users can take:

- always use varied and complex passwords for all your accounts (see earlier notes)
- check the accuracy of bank accounts continually and resolve any discrepancies immediately
- only provide personal information on sites that have 'https' in the web address or have the padlock icon in the web browser
- don't provide personal information to any unsolicited requests for information; this is often a sign of phishing
- don't open emails or attachments from unknown senders
- delete any messages from your spam folder on a regular basis
- report any suspicious phishing activity to the company that is used by the perpetrator
- only download software from sites that can be trusted.

Cloud security

Several computer (especially tablets and laptops) and mobile phone manufacturers encourage customers to store or backup their files on a medium known as the **cloud**. Users purchase cloud storage and can then access all their files (for example, photos, videos, music or e-books) from any device anywhere in the world. This has obvious advantages:

- you don't need to carry memory sticks around with you if you want to access your files away from home
- you don't have to pay for large storage capacity on your computer/tablet or mobile phone
- because the cloud is controlled by external companies, they will ensure that your files are backed up and therefore reduce the possibility of losing irreplaceable data
- the ability to synchronise (sync) files ensures they are automatically updated across all devices; this means that the latest version of a file saved on a desktop PC, for example, is also available on other devices, such as a smartphone
- cloud storage is also ideal for collaboration purposes; it allows several users to edit and collaborate on a single file or document – there is no need to worry about tracking the latest version or which user made the changes.

In spite of all these obvious advantages, there are still security worries about using cloud storage. The main fears are data security and data loss.

Data security

Companies that transfer vast amounts of confidential data from their own systems to a cloud service provider are effectively relinquishing control of their own data security. This raises a number of questions:

- What physical security exists regarding the building where the data is housed?
- How good is the cloud service provider's resistance to natural disasters or power cuts?
- What safeguards exist regarding personnel who work for the cloud service company? Can they use their authorisation codes to access confidential data for monetary purposes?

Data loss

There is a risk that important and irreplaceable data could be lost from cloud storage facilities. Actions from hackers (gaining access to accounts or pharming attacks, for example) could lead to loss or corruption of data. Users need to be certain sufficient safeguards exist to overcome these potentially very harmful risks.

In late September 2014, three breaches of security involving two of the largest cloud service providers showed why many of the above fears make people a little nervous of using this facility to store their important files:

- the XEN security threat, which forced several cloud operators to reboot all their cloud servers; this was caused by a problem in the XEN **hypervisor** (a hypervisor is a piece of computer software, firmware or hardware that creates and runs virtual machines)
- a recent case where a large cloud service provider permanently lost data during a routine backup procedure
- the celebrity photos cloud hacking scandal, where over 100 'interesting' photos of celebrities were leaked; hackers had gained access to a number of cloud accounts, which enabled them to publish the photos on social networks and to sell them to publishing companies.

All of the reasons above have made individuals and companies nervous about using cloud service providers. A 'game' between hackers and owners of online service companies continues to simmer. Considerable amounts of advice have been given in this chapter. Provided users are vigilant in their use of any device connected to the internet then the possibility of being a victim of cybercrime is considerably reduced.

9 Audiences

In this chapter you will learn about:

- how to tailor ICT solutions according to the audience
- copyright legislation
- legal, moral, ethical and cultural implications of ICT solutions
- policing of the internet.

This chapter will consider the importance of researching your audience before an ICT solution is implemented – this ranges from presentations through to actual ICT systems which run companies. No matter how large or small the task, consideration of the people involved with the presentation or full solution must be taken into account.

The legal, moral, ethical and cultural aspects of ICT solutions will also be considered together with the age-old question 'Should the internet be policed?'

At the end of the chapter, you should have some idea about the importance of the above topics, particularly in the multicultural and litigation-driven society we now live in.

9.1 Audience appreciation

When planning and creating ICT solutions, it is important to consider the audience who will either use or take part in the solution. The following list shows a number of factors that should be considered – not all of them are relevant to every proposed solution, of course.

- The age of the target group (young children will have a different appreciation and response compared to a more mature group of adults, for example).
- The experiences of the audience (a board of company directors would expect a different approach compared to an audience composed of teenage school children).
- The expectation of the audience (for example, if you are advertising or giving a presentation on a new restaurant, an older audience would expect to see fine wines and good waiter service; whereas a group of students would be more interested in pizzas and fast counter service).
- Knowledge of the audience (for example, graduates in maths would expect to see a different approach to a solution than a group of history students).

When starting to look at the ICT solution, some or all of these factors need to be taken into account. Some research needs to be done first to find out about the target audience. This could be done by:

- interviewing a cross section of the target group to find out how to engage the audience (if this involves a major ICT solution, then this may have to involve many of the techniques that were described in Chapter 7)
- giving out questionnaires to people in the target group to find out their background, interests, and so on, so that the final solution can be tailored to meet the full expectation of the audience
- carrying out market research – this could involve the two techniques described above, but would certainly involve a more sophisticated and in-depth analysis of the data received (it would all depend on how large the 'affected' audience is likely to be).

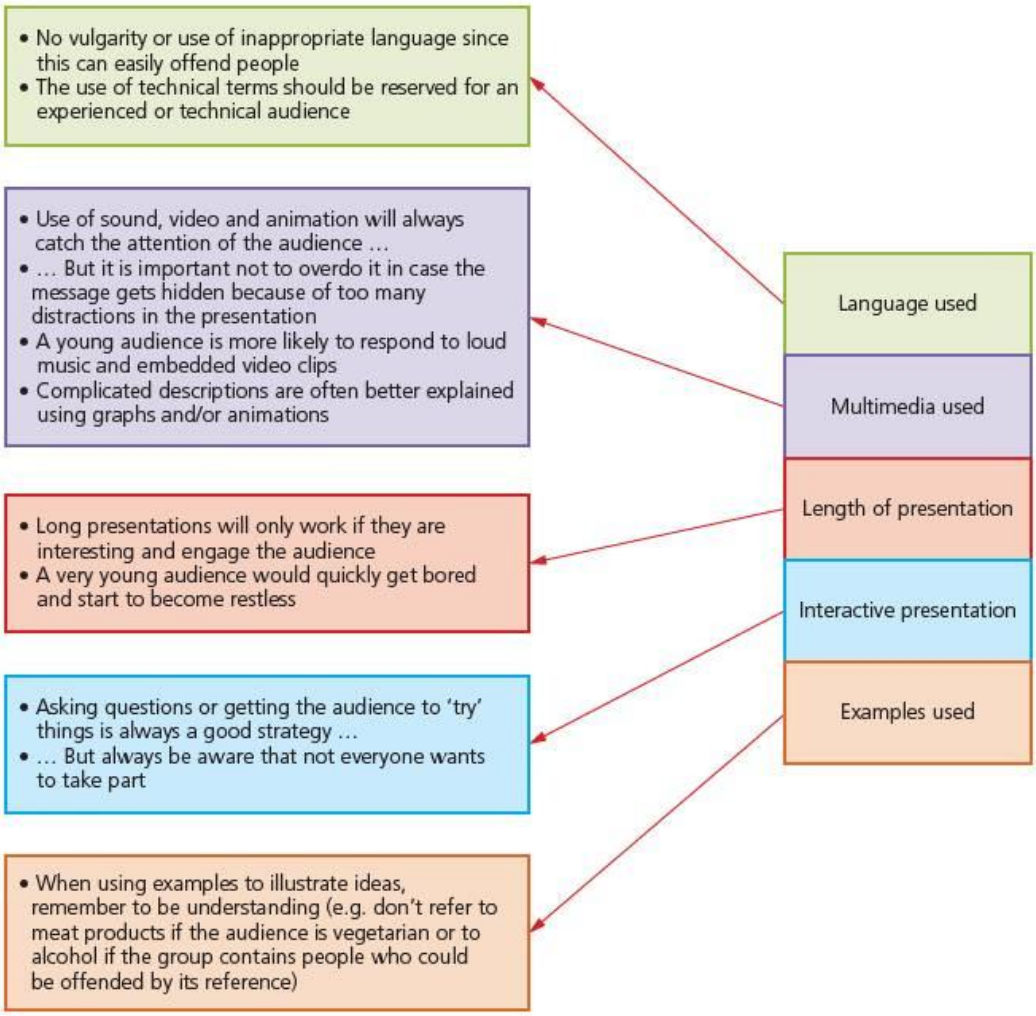
9.1.1 Giving a sample presentation to an audience

Let us now consider a phone company who market a number of different mobile phones. The company has decided to do two presentations regarding the sales and features of the four different mobile phones they market and sell:

- one presentation is to be given to the sales team who will receive different bonus payments depending on the phone sold
- a second presentation is to be given to a potential group of customers.

How would these two presentations differ? The first group (the sales team), will have technical knowledge and will be interested in the profitability of each sale. The second group (end-users), will only be interested in the price and the features found on each phone.

The language used, the need for multimedia, the length of the presentation, the need for audience participation (an interactive approach) and the examples used to illustrate certain points are all key factors when writing the presentations. Let us look at each of these in turn:



Now let us consider our mobile phone presentation.

The data to be used in the two presentations is based on the following:

- sales of each phone over three years
- selling (retail) price of each phone
- percentage profit made on each phone
- how the prices and profit margin changed over the three-year period

Table 9.1

	2014		2015		2016	
	Retail price	% profit	Retail price	% profit	Retail price	% profit
Neophone	$400	35%	$440	37%	$450	40%
Rappia	$525	29%	$560	31%	$590	30%
Wintry	$350	40%	$380	40%	$400	41%
Samstalk	$650	25%	$700	27%	$750	30%

- features of each phone (do they have a camera, memory size, do they have a touch screen and do they have an MP3 player).

It is worth remembering here that customers would be more receptive to colours, supporting images and special effects (e.g. slide transitions). Whereas the sales team (who already know about selling the phones) simply want to know the facts. Customers, on the other hand, really want to be 'entertained' by the phone presentation.

Table 9.2

	Mobile phone features			
	Camera	Memory	Touchscreen	MP3 player
Neophone	√	16 GB	√	√
Rappia	√	32 GB	X	√
Wintry	√	16 GB	X	X
Samstalk	√	64 GB	√	√

Exercise 9a

Produce the two presentations for the scenario given in Section 9.1.1:

- for the marketing and sales team
- for a group of customers.

Using your knowledge from Section 9.1 and from Chapter 19 (Presentations), consider how to present the information in Table 9.1 and Table 9.2 to the two groups. Also consider what information you might want to have in each presentation and any additional information you might need.

For the mobile phone features, you may like to use icons such as:

-  built-in camera
-  memory
-  touchscreen
-  MP3 player.

Additional example

This second example (which is the introduction to Exercise 9b) considers producing a presentation on the 'increase in world population over the next ten years'. The presentation is to be given to two different audiences:

- adults
- children of primary school age (5 to 11 years old).

We have already covered aspects of an adult audience. What needs to be considered when presenting to young children?

- careful consideration needs to be given to font type used; a large font size is more likely to make young children interested
- bright colours will keep their attention
- use of the correct language (for example, to say 'the world population is 7.1 billion for which China accounts for 1.4 billion' is acceptable to adults; young children won't understand the figures or the statistics so the presentation would need to say 'the world's population is very big; for example, 60 million people live in the UK. But some countries, such as China, are much bigger than this', and so on)
- use of lots of images to make it amusing (and have sound effects as well)
- use of slide transitions and animation to keep their attention.

Exercise 9b

Produce two slide presentations on 'changes to the world population'. One presentation is aimed at an adult audience and the other is aimed at a very young audience (5 to 11 years). Write down your reasons for the features of each presentation you produce.

It is important to remember that the example given in Section 9.1.1 was a presentation to two very different groups of people. However, the audience may be the actual users of the ICT solution. To meet the audience requirements in this case also requires a number of key considerations, for example:

- how skilled is the workforce (the interface might need to be icon-driven if the staff are either computer-illiterate or not very skilled)
- how old is the workforce (is the interface appropriate for all the age ranges who will use the system)
- are any of the staff disabled (different disabilities require different methods to allow them to interface with a computer system)?

Exercise 9c

A small company employs a workforce where 35% of the staff are disabled, have learning difficulties or come from an ethnic minority. The company markets various food products.

- 10% of the staff have little or no hand or arm movement.
- 10% of the staff have learning difficulties.
- 15% of the staff come from ethnic minorities.

Write an article on the features needed in a computer interface to cope with the range of different staff that work within the company.

9.2 Legal, moral, ethical and cultural appreciation

9.2.1 Software copyright and privacy

Software is protected by copyright laws in much the same way as music CDs, videos and articles from magazines and books are protected.

When software is supplied on CD or DVD there are certain rules that must be obeyed. It is illegal to:

- make a software copy and then sell it or give it away to a friend or colleague
- use software on a network or in multiple computers unless a licence has been acquired to allow this to happen
- use coding from the copyright software in your own software and then pass this software on or sell it as your own without the permission of the copyright holders
- rent out a software package without permission to do so from the publishers
- use the name of copyrighted software on other software without agreement to do so.

Software **piracy** (illegal copies of software) is a big issue amongst software companies. They take many steps to stop the illegal copying of software and to stop illegal copies being used once they have been sold. There are a number of ways software is protected either by making the installer agree to certain conditions or by methods which require the original software to be present for it to work:

- when software is being installed, the user will be asked to key in a unique reference number or **product key** (a string of letters and numbers) which was supplied with the original copy of the software (for example: 4a3c 0efa 65ab a81e)
- the user will be asked to click 'OK'/'I AGREE' or put a cross in a box to agree to the licence agreement before the software continues to install
- the original software packaging often comes with a sticker informing the purchaser that it is illegal to make copies of the software; the label is often in the form of a **hologram** indicating that this is a genuine copy
- some software will only run if the CD-ROM, DVD-ROM or memory stick is actually in the drive; this stops illegal multiple use and network use of the software
- some software will only run if a **dongle** is plugged into one of the USB ports.

Note: A dongle is a small device, usually plugged into one of the computer's USB ports. It is used to allow wireless communications with devices, such as a keyboard, and for the use of protected software (e.g. it may contain important files and the software will only run if the dongle is plugged into the computer).

The Federation Against Software Theft (FAST) was set up in the UK many years ago to protect the software industry against piracy. FAST prosecutes organisations and individuals who are involved in any copyright infringements. There are legal penalties for anyone found guilty of such infringement.

Similar organisations exist in many countries to globally protect software from piracy. The following extract is a typical example of how strict the anti-piracy laws are in many countries:

> **TRADERS FINED $100,000**
>
> Two eBay traders (from the US) agreed this week to pay a total of $100,000 in damages after they were caught selling illegal copies of Norton security software. The SIIA settled the case against the two traders who also agreed to stop selling illegal software and provided SIIA with records identifying their customers and suppliers.

Reproduced with the kind permission of out-law.com.

9.2.2 Legal, moral, ethical and cultural implications

Note: it is also worth looking at Chapters 5, 8 and 10 for further information on the legal implications of ICT.

Definitions:

- **Legal** covers the law; whether an action is punishable by law.
- **Morality** governs the private and personal interactions between people and is usually determined by the person concerned.
- **Ethics** governs professional interactions, for example, codes of behaviour practised by a society or group of people sometimes going against an individual's own sense of morality.
- **Culture** refers to the attitudes, values and practices shared by a society or group of people.

Essentially, anything which breaks the law is termed *illegal*. Examples from ICT would include copying software and then selling it without the permission of the copyright holders. This was covered in Section 9.2.1.

Morality covers the human desire to distinguish between right and wrong. The only problem here is that culture can get in the way. What may be immoral in some cultures is regarded as acceptable practice in other cultures. Because something is immoral, it isn't necessarily illegal (and vice versa). Altering websites or creating fake websites is not in itself illegal; provided the person who carries out the act doesn't try to gain from their actions – it is simply an immoral act since it can cause distress to others who aren't aware that it was simply a harmless prank. As soon as they try to obtain personal and financial data then it becomes an illegal act. Some people regard hacking as simply immoral – this again ceases to be true if the act of hacking leads to breaking national security, or financial gain or leads to revealing personal information which leads to distress. It can be a very thin dividing line between an immoral act and an illegal act.

Unethical behaviour is essentially breaking a code of conduct. For example, if somebody works for a software company and passes on some of the ideas to a rival company, this would be regarded as unethical behaviour. Unless the software passed on is part of national security, then it isn't actually illegal to do this.

The importance of culture is less clear-cut. Writing software games that make fun of religion could be seen by certain people as unacceptable behaviour – but some cultures would find it funny and wouldn't understand why it was seen as offensive. When writing computer games, for example, programmers need to be careful that they don't include items which some cultures would find offensive or obscene. Again, this may not be seen as unethical and certainly not illegal, but nonetheless can cause distress.

Exercise 9d

Suppose John works for a company during the day that develops and markets software for use by car manufacturers. In the evening, he works with a small team who write software for computer games. Consider which of the following can be termed unethical, immoral or illegal (it is possible some things may be regarded as all three):

1. John uses some of the software routines from his day job when writing computer games.
2. John claims that the software routines he uses from his day job were all written by himself.
3. John has some of his software written overseas, but only pays them a very low wage to do the work.
4. John writes some of his computer games using the computer systems in his day job.
5. To help advertise his computer games, John hires a 'hacker' who breaks into websites so that 'pop ups' appear which advertise the games free of charge.
6. Some of the games software written by John's company makes fun of people who have certain disabilities.
7. Some of the games that John writes collect information from the user's computer and send the data back to John's computer.

Once you have decided the answers to the above seven statements, write down other activities which fall into the illegal, unethical or immoral category. For each activity, give reasons why they fall into one or more of these categories.

At the end of Exercise 9d you should have come to the following conclusions: statements 1, 2 and 4 are unethical; statements 2, 3 and 6 are immoral; statements 5 and 7 are illegal. But this can vary in some countries; for example, statement 1 may be illegal in certain parts of the world.

9.2.3 Should the internet be policed?

This is a question which continues to cause much discussion. Recent events in hacking (e.g. the hacking of Sony Films in USA) and in terrorism (e.g. the 2015 terrorist attacks in France) have brought increasing pressure from many people to start policing the internet. Those that support freedom of speech argue that the internet only works because it isn't policed. Many security departments and governments believe that the hacking and terrorism attacks could have been stopped by having tighter laws (allowing them to 'eavesdrop' on any data transmission on the internet). There are many points that support both sides of the argument.

Arguments in favour of some form of internet control

- It would prevent illegal material being posted on websites (e.g. racist comments, pornography, terrorist activities, and so on).
- People find it much easier to discover information which can have serious consequences (e.g. how to be a hacker, how to make a bomb, and so on); although this can be found in books, it is much easier for a novice to find the required information using a search engine.
- Some form of control would prevent children and other vulnerable groups from being subjected to undesirable websites.
- Some form of control would stop incorrect information being published on websites.

Arguments against some form of internet control

- Material published on websites is already available from other sources.
- It would be very expensive to police all websites and users would have to pay for this somehow.
- It would be difficult to enforce rules and regulations on a global scale.
- It can be argued that policing would go against freedom of information/ speech.
- Many topics and comments posted on websites are already illegal and laws already exist to deal with the offenders.
- Who is to decide what is illegal or offensive – many things are only offensive to certain people (e.g. religious comments) but not to the majority.

Having read the arguments for and against policing, you may wish to enter into your own debate as to whether freedom of speech is so important that the risks of more internet legislation would be too damaging. However, you might argue that losing some of your freedom of speech is a small price to pay for your own physical safety.

10 Communication

In this chapter you will learn about:

- communication constraints when using emails
- email groups
- cloud storage
- spam
- the internet
- intranets
- the world wide web (www)
- blogs, wikis and social networking sites
- searching the internet for information.

This chapter covers certain aspects of using the internet. We will consider rules and regulations when sending emails and also look at several features of the internet. In particular, we will define and explain many of the internet terms used and how to search for information on the internet. The chapter also considers the differences between the internet, the world wide web and intranets.

10.1 Communication with other ICT users using email

10.1.1 Constraints

Emails are now one of the most common ways of communicating between people. However, there are many rules we need to follow to ensure the security of the messages sent and also to prevent people from writing things that are regarded as unacceptable. The first part of this chapter considers these constraints.

Laws

Many countries have laws to protect people against the misuse of emails. The following diagram is a guideline to the rules that most countries require companies and individuals to abide by when sending out emails.

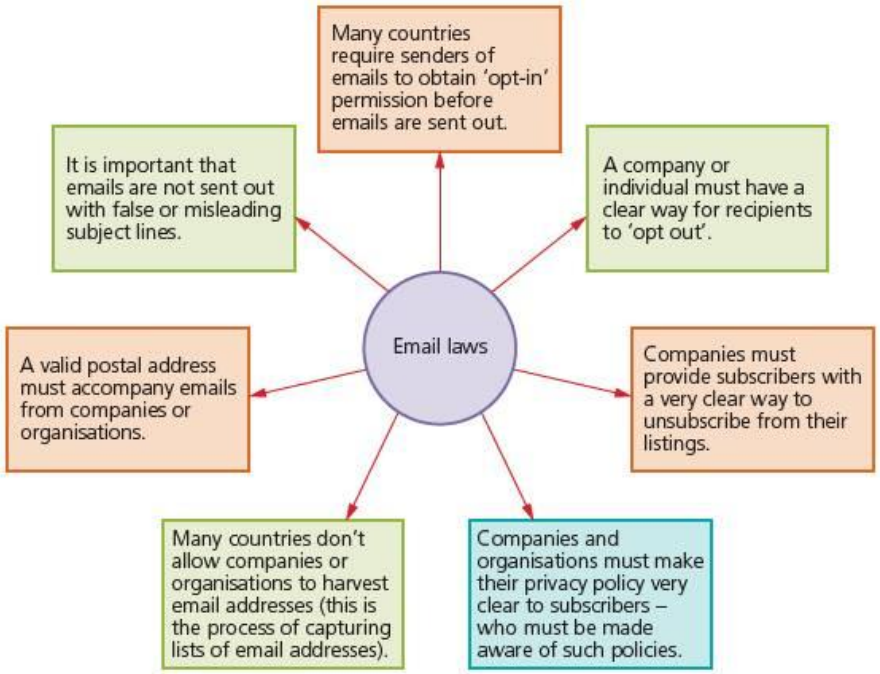


Figure 10.1 Email laws

Acceptable language

The language used by people when writing emails must lie within an acceptable code of practice. The following is a list of unacceptable content to be used in emails, text messages and online forums:

- obscene images
- language that is regarded as abusive, profane, inflammatory, coercive, defamatory or blasphemous
- racist, exploitative, violent messages
- use of illegal materials in messages.

This list doesn't cover everything but gives some idea of what is not acceptable when posting messages or items on the internet. In many countries there are very stiff penalties for going outside the above boundaries, and it is not regarded as adequate that recipients can simply delete images or messages.

It is essential that anyone writing emails or posting messages on, for example, bulletin boards, is aware of the above constraints.

Copyright

It is very important to realise that emails are subject to copyright laws. Just because it is relatively easy to forward an email does not mean it is always legal to do so. This is also true of any attachments sent with an email.

As with web pages, the copyright in an email is determined by its content.

Printing, copying or forwarding emails is generally not considered a breach of copyright unless the sender has indicated clearly that the message is confidential or the subject of copyright law. It is important that the recipient checks this out before forwarding it on to somebody else. Most companies or organisations will clearly set out their policies on sending emails and the material that they contain. This will be particularly true if the sender's email address is part of the company's name, for example A.N.User@company_name.com. Emails and attachments from companies and organisations will usually contain a copyright statement, such as:

> Any dissemination or copying of this email or attachment is strictly prohibited unless you are the intended recipient or are responsible for delivering the message to the intended recipient. If you have received this email in error, please let us know and then delete the original email and any attachments.

It is common for the message to then make some statement that the views and opinions in the email may not represent those of the company, and that the contents may be subject to disclosure under the Freedom of Information Act. Companies are clearly very concerned about any potential risk of copyright infringement.

Security and password protection

It is very important to consider the security of emails. Many security aspects have been covered elsewhere in this book but some of the factors to consider are repeated here for completeness.

Some methods of increasing the security of emails include:

- using strong passwords when logging on to your email (for example, the name of your pet dog is a weak password; strong passwords contain a combination of letters, numbers and other symbols: Sy12@#TT90kj=0 would be regarded as a strong password)
- changing passwords on a regular basis

- using spam filters to remove suspicious emails to a 'junk folder' or even to block the email entirely
- running anti-virus and anti-spam software at all times on your computer to protect against emails from unknown or malicious sources.

Emails are said to be vulnerable to both **passive** and **active** attacks. Passive attacks include the release of email material to other users without your consent. Active attacks involve the modification of your messages or even denial of service (i.e., overloading your system by sending thousands of emails, which basically 'clogs up' your computer and makes internet access almost impossible). Active attacks can also involve viruses or phishing attacks (these are covered elsewhere in the book).

Netiquette

Netiquette is a shortened form of the phrase **internet etiquette**, which refers to the need to respect other users' views and display common courtesy when posting views in online discussion groups or when sending out emails. It is very important to consider what you write always since the reader can't see your facial expressions or body language. What may have been intended to be humorous could offend somebody if they misunderstand your message and make the wrong conclusions. Always be aware of this when posting messages or sending emails.

There are a number of rules governing netiquette – one such source is *The Core Rules of Netiquette* by Virginia Shea (published in 1994); but the following diagram gives the reader some idea of what constitutes netiquette.

Figure 10.2 Rules of netiquette

10.1.2 Spam

Any unsolicited email sent over the internet is regarded as **spam**. It is often sent to multiple recipients and can range from being simply annoying to dangerous – spam can contain viruses or be part of a phishing scam (see earlier chapters). The origin of the word is open to debate: it ranges from the name of an old war-time foodstuff called spam to a word used in an old BBC Monty Python television comedy sketch ('spam, spam, spam, spam, spam, spam…' – a word repeated many times!).

Spam can affect many online operations (for example, YouTube) where links (called 'spambots') are posted within videos that send users to another website.

While some regard spam as a cheap way of advertising to many people at the same time, most people consider it to be a big nuisance. The main disadvantages are:

- it uses up people's time
- it generally annoys people
- it uses up valuable bandwidth on the internet, slowing it down
- it can have viruses attached or even be part of a phishing scam
- it can clog up users' inboxes.

Spam is not just a problem for computer users – it can also affect mobile phones. In this case it is usually text messages being send to multiple phones. They are sometimes referred to as 'spasms' (spam SMS) – at the basic level they just annoy people, but in some countries or with some mobile phone providers, users are charged for each message they receive. It then becomes more than just an annoyance! (Look back at Chapter 8 for ways to prevent spam.)

10.1.3 Email groups

Email groups are used for a number of purposes:

- it is easier for a user to send out multiple emails if the addresses are all grouped together under a single name; the user only needs to use that single name in the 'to' box
- companies and organisations can group people together for marketing purposes, for example according to age, ethnicity, hobbies, favourite music and so on – this means that each email can target specific groups
- 'spammers' can create email groups by buying addresses of people from certain companies or from software that 'raids' address books on computers or email companies – this means that several thousand people can be sent spam by simply pressing the <enter> key
- companies use email groups to set up meetings (for example, for a video conference) to ensure that everybody is always invited to attend – it would be easy to forget a person if the email addresses were all typed in individually; this way you can be sure all the correct people are sent messages.

10.2 Effective use of the internet

10.2.1 The internet

The **internet** is a worldwide collection of networks that allows users to:

- send and receive emails
- chat online (using text, voice and/or video)

- transfer files from computer to computer (using file transfer protocols)
- browse the world wide web.

In 2015 it was estimated that over three billion people use the internet across the world. The internet isn't actually owned by any single person or organisation. It is a concept rather than something tangible (that is, something that can be touched) and relies on a physical infrastructure that allows networks to connect to other networks.

The **world wide web** (the web, or www) is only *part* of the internet, which users can access by way of a **web browser**. It consists of a massive collection of web pages and has been based on the **hypertext transfer protocol (http)** since 1989. The world wide web is a way of accessing information over the medium known as the internet; the two terms 'www' and 'internet' are clearly not the same thing and should not be confused.

10.2.2 Intranets

Many companies use an **intranet** as well as the internet. An intranet is defined as 'a computer network based on internet technology but designed to meet the internal needs for sharing information within a single organisation or company'. *Access* to an intranet is usually confined to a company or organisation and, unlike the internet, is not available to the general public.

Intranets reside behind a **firewall** and are only accessible:

- internally to members of the company, or
- to people given various levels of access who are external to the company (see later).

There are a number of reasons for adopting intranets rather than using the internet:

- intranets are safer since there is less chance of external hacking or viruses
- it is possible to prevent external links to, for example, certain websites
- companies can ensure that the information available is specific to their needs
- it is easier to send out sensitive messages in the knowledge that they will remain within the company
- intranets offer better bandwidth than the internet, thus there are fewer connection limits than with the internet (that is, the number of bits per second that can be transmitted are usually higher within an intranet)
- it is possible to create **extranets** that allow intranets to be extended outside the organisation but with the same advantages as an intranet; this allows, for example, trading partners to have controlled access to some of the information (commercially-sensitive information is password protected).

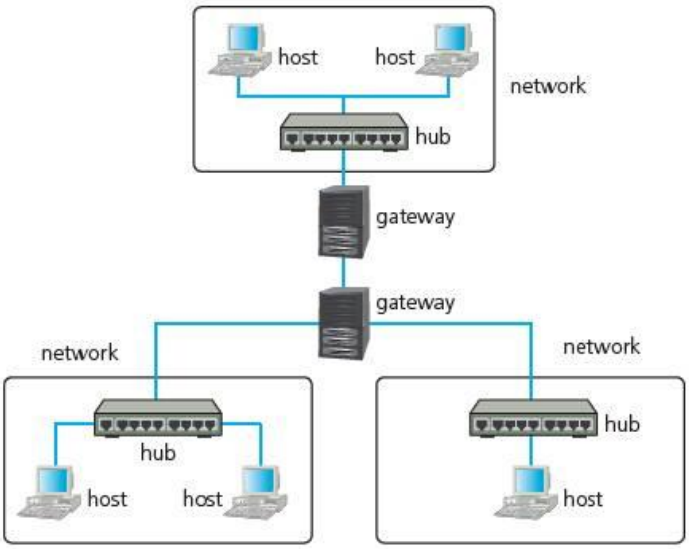


Figure 10.3

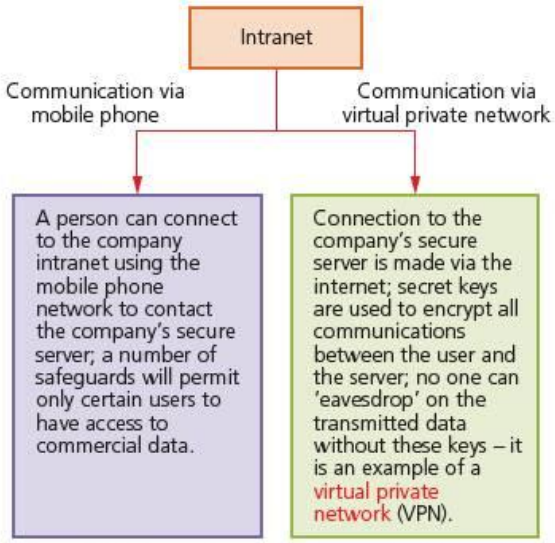


Figure 10.4 Connecting to an intranet though a mobile phone network or virtual private network

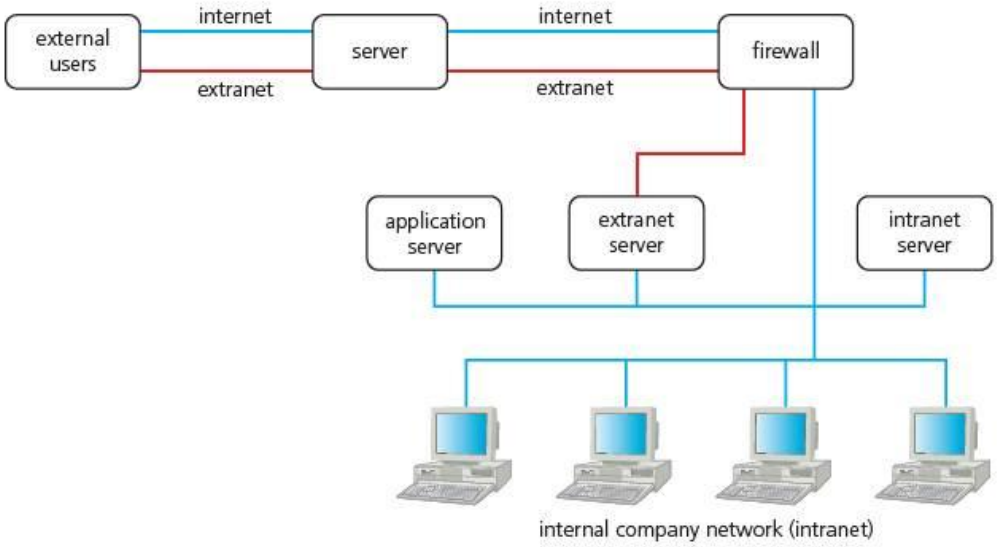


Figure 10.5 How intranets, extranets and the internet can be connected together

What are the differences between the internet and an intranet?

- The term 'internet' comes from the phrase: **inter**national **net**work.
- The term 'intranet' comes from the phrase: **intra**nal restricted access **net**work.
- An intranet is used to give local information relevant to the company or organisation whereas the internet covers topics of global or general interest.
- It is possible to block certain websites using the intranet; while this is also possible with the internet, it is more difficult.
- An intranet requires password and user ID entry and can only be accessed from agreed points/computers; the internet can be accessed from anywhere in the world provided the user has an ISP account.
- An intranet is behind a firewall, which gives *some* protection against hackers, viruses, and so on; this is more difficult to do with internet access since it is open on an international scale.
- The internet can be public access, whereas intranets tend to be private access.

10.2.3 Cloud storage

Cloud storage is a method of data storage where data is stored on offsite servers – the physical storage covers hundreds of servers in many locations. The same data is stored on more than one server in case of maintenance or repair, allowing clients to access data at any time. This is known as **data redundancy**. The physical environment is owned and managed by a hosting company.

Security aspects of **cloud storage** were discussed in Chapter 8.

There are three common systems:

- **Public cloud**: this is a storage environment where the customer/client and cloud storage provider are different companies.
- **Private cloud**: this is storage provided by a dedicated environment behind a company firewall; customer/client and cloud storage provider are integrated and operate as a single entity.

- **Hybrid cloud**: this is a combination of the two previous environments; some data resides in the private cloud while less-sensitive/less-commercial data can be accessed from a public cloud storage provider.

Instead of saving data on a local hard disk or other storage device, a user can save their data 'in the cloud'. The advantages and disadvantages of doing this will now be discussed.

Advantages

- Customer/client files stored in the cloud can be accessed at any time, from any device, anywhere in the world, provided internet access is available.
- There is no need for a customer/client to carry an external storage device with them, or even to use the same computer, to store and retrieve information.
- The cloud provides the user with remote backup of data with obvious advantages to alleviate data loss/disaster recovery.
- If a customer/client has a failure of their hard disk or backup device, cloud storage will allow recovery of their data.
- The cloud system offers almost unlimited storage capacity.

Disadvantages

- Security aspects of cloud storage were discussed in Chapter 8.
- If the customer/client has a slow or unstable internet connection, they could have problems accessing or downloading their data/files.
- Costs can be high if a large storage capacity is required; it can also be expensive to pay for high download/upload data transfer limits with the customer/client internet service provider (ISP).
- The potential failure of the cloud storage company is always possible – this poses a risk of loss of all backup data.

10.2.4 General internet terms

A number of terms have been introduced in this chapter – this section considers the definition of these terms.

Hypertext transfer protocol (http and https)

Hypertext transfer protocol (http) is a set of rules that must be obeyed when transferring data across the internet. Protocols are sets of rules agreed by the 'sender' and 'recipient' when data is being transferred between devices. When a web page is being accessed, entering 'http://' at the front of an address tells the web browser that http rules for communication are to be obeyed.

If http is omitted from the address, most web browsers now default to http.

When some form of security (for example, SSL or TLS) certification or encryption is used (refer to Chapter 8) then the protocol is changed to https (this is often seen as the padlock symbol). The letter 's' after http refers to 'secure'.

Because of encryption, it is slower to use https than http, so it is usually only adopted when sensitive or private data is being transferred across the internet.

Web browsers and URLs

A **web browser** is software that allows a user to display a web page on their computer screen. They interpret or translate the HTML (hypertext markup language – see later chapters) from websites and show the result of the translation. This can often be in the form of videos, images or sound. Most web browsers share the following features:

- they have a 'home' page
- they have the ability to store a user's favourite websites/pages
- they keep a history of the websites visited by the user
- they give the ability to go backward and forward through websites opened
- they have **hyperlinks** that allow users to navigate between web pages; these hyperlinks are shown as blue underlined text or use a small picture, such as a pointed finger  , under a phrase or image. By clicking on these hyperlinks the user is sent to another website or web page.

Web browsers use **uniform resource locators (URLs)** to access websites, retrieve files and so on. They are represented by a set of four numbers, for example 109.108.158.1 (i.e., http://109.108.158.1).

However, this is not very user friendly, and an alphanumeric format is usually used instead:

protocol://website address/path/filename

where:

- **protocol** is usually http or https
- **website address**:
  - domain host (www)
  - domain name (name of website)
  - domain type (.com, .org, .co, .net, .gov)
  - sometimes a country code is given (.uk, .us, .de, .cy)
- **path**, which is a web page (if omitted then root directory of website)
- **filename** is the item on the web page

For example, **http://www.hoddereducation.co.uk/igcse_ICT**

An error will occur if any part of the URL is incorrect. Most frequently, error page 'HTTP 404' will display on the computer screen.

The web browser translates the web server name into an IP address (for example, 109.108.158.1). The HTML is returned and is shown as a correctly formatted page on the screen.

File transfer protocol (ftp)

File transfer protocol (ftp) is a network protocol used when transferring files from one computer to another computer over the internet. It is similar to http (used for the transfer of web pages and data) and smtp (simple mail transfer protocol – used when transferring emails); ftp is an application protocol for the transfer of files across the internet.

Web browsers can be used to connect to an ftp address in much the same way as you would connect to an http address, for example ftp://username@ftp.example.gov/ .

Internet service provider (ISP)

An **internet service provider (ISP)** is a company that provides users with access to the internet. It is normal to pay a monthly fee for this service. When a user registers with an ISP, an account is set up and they are given login details that include a user ID and password.

An ISP has the equipment and telecommunications line access required to have internet access – usually broadband connections, which use copper cables, or, more recently, fibre-optic cables.

So what is the difference between an ISP and a web browser?

- ISPs provide the user with access to the internet for a monthly fee
- web browsers allow a user to view web pages.

10.2.5 Blogs, wikis and social networking sites

Blogs

Blogs (**web logs**) are personal internet journals where the writer (blogger) will type in their observations on some topic (for example, a review about the latest movie release) and perhaps provide links to some relevant websites.

Blogs tend to range from minor projects (such as the performance of a rock star) through to important social issues. However, the comments made on blogs are **not** immune from the law: bloggers can still be prosecuted for writing offensive material.

Features of blogs:

- updated on a regular basis by the author
- usually organised in reverse chronological order (most recent to least recent entry)
- normally public – anyone can read them
- entries normally come from a single author
- other internet users can't change blogs – they can only read them.

Microblogs are similar to blogs but are most often used on social networking sites to make short, frequent posts. The posts can be done using instant messaging, emails or other social networking vehicles (such as tweets). Social networking sites use microblogs to allow members to update their personal profiles, for example.

Another version is a **b-blog** – short for business blog – which is used by businesses to promote themselves on the internet.

Wikis

Wikis are web applications or websites that allow users to create and edit web pages using any web browser. A wiki will support hyperlinks and uses a very simple syntax (known as wiki markup) to create pages. They are often described as 'web pages with an <edit> button'.

Features of wikis:

- anyone can edit, delete or modify the content
- many authors can be involved in a wiki
- it is possible to organise a page any way that the author(s) wish(es)
- shows/keeps track of all entries – i.e. it stores a document history
- can be easily edited using a web browser
- allows large documents to be seen by many people – it is easier than emailing several people.

Social networking sites

Social networking sites focus on building online communities of users who share the same interests and activities. They enable people to share photos, videos and music, hobbies, favourite eating places, and so on. The members do this by creating public profiles and thus form 'relationships' with other users. The dangers of such sites were covered earlier in Chapter 8.

Features of social networking sites:

- each member is provided with free web space
- each member can build their own private and public profiles
- it is possible to upload content such as text messages, photos and videos
- it is possible to 'write on each other's wall'
- members are given free instant messaging and video chatting
- it is possible to email other members within the community
- members can create pages where they can post photos, articles, and so on
- it is possible to invite people to become friends
- members have control over who can access their private or personal data.

10.2.6 Searching the internet for information

One of the most useful and powerful aspects of the internet is the ability to easily search for vast amounts of information on almost any given topic. There are basically two ways to locate information:

- The first is to type in the URL if you know the name of the website you wish to access.
- If you don't know where to find the information you are looking for, the second method is to use a **search engine**.

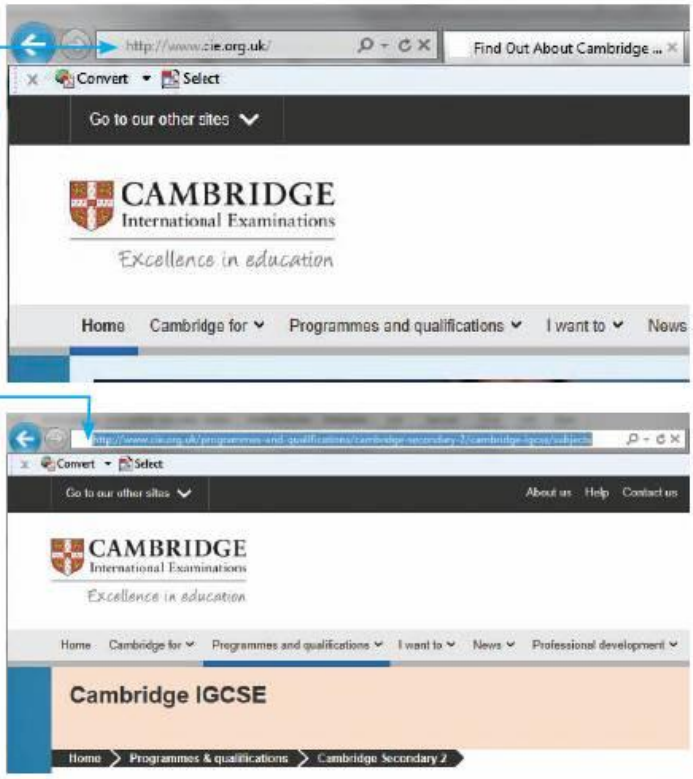
Opening a website from a URL

As discussed earlier in the chapter, the URL contains the protocol, site address and file name. If you type http://www.cie.org.uk in to a web browser as shown here, you will go to the home page for the website.

If you know the URL for a page within the website, you can type the full entry into the web browser to get a particular page. For example, if you want the IGCSE subjects page within the website, you could type in the full URL: http://www.cie.org.uk/programmes-and-qualifications/cambridge-secondary-2/cambridge-igcse/subjects/ to get this page.

If you want to use this page frequently, you can add it to your 'favourites', which saves you having to type in the URL every time.

It is also possible to search through the website using the navigation tools until you find the web page you are looking for.

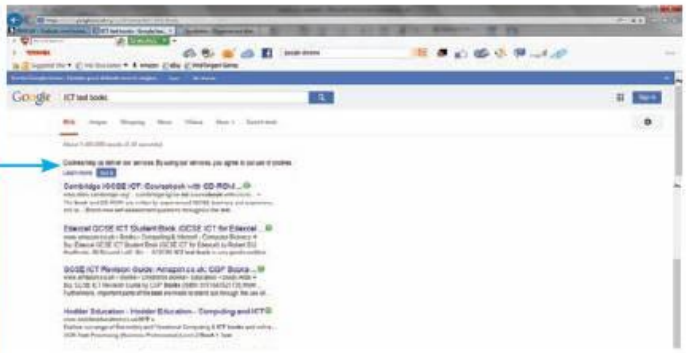


Search engines

Search engines are useful if you don't know the URL of the website or if you want to find some information but don't know where to look. Many search engines exist, and they search for websites using a variety of methods, but they all have one common underlying feature: they use the words entered in the search box and look up in their database of web pages to find out which of them match your search string.

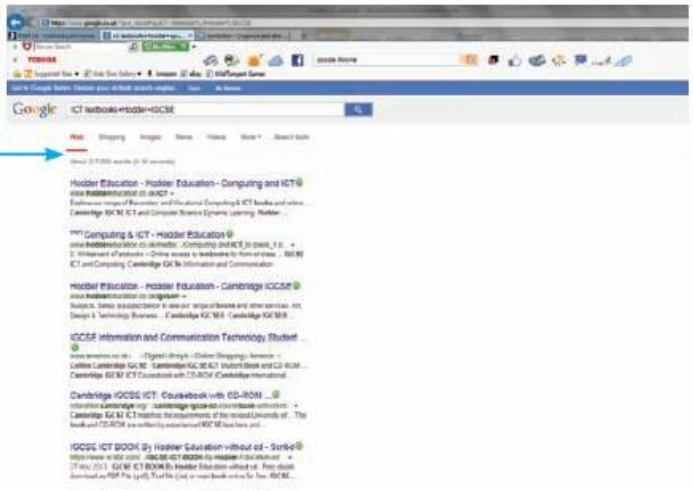
Obviously, the more detailed or specific your search string, the more accurate the results (known as 'hits') will be. For example, if we type **ICT textbooks** into a typical search engine, the following options will appear:

As you can see about 1.5 million 'hits' or web pages have been found. This is a lot of information. We could narrow down the search by now typing in **ICT textbooks+Hodder+IGCSE** – we now get a much reduced selection:



We now have reduced the number of web pages to 217 000, which is a vast reduction. However, the search can be further refined using the advanced search option.

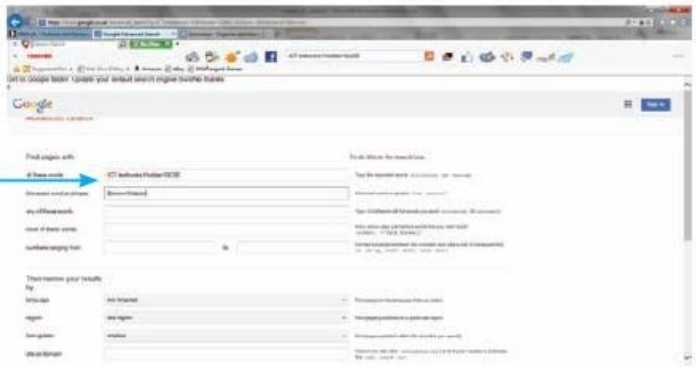
```
Add this text if known and it will
search for both words together, not
just for either word.
```



The result is now only about 2000 hits.

Once the information is found it can then be saved or used as follows:

- saved as a favourite (as described earlier) and accessed when required
- by adding hyperlinks in a document, so that this web page can be accessed when required
- by using 'Print Screen' (or the equivalent – it varies from computer to computer) and then pasting the saved information into a word processor page
- copy and pasting the information into another document.



It is important to acknowledge your sources of information when doing this, both to avoid plagiarism and because the information may be subject to copyright.

As we have already said, the internet is a vast and very useful source of information, but it is important to be aware of its disadvantages as well its advantages.

Advantages

- Information on the internet tends to be up-to-date since it is quicker and easier to amend web pages than, for example, to reprint books.
- The internet has vast, almost limitless, amounts of information.
- Searching for information using a search engine is fast and easy.
- People can look for information in the comfort of their own home – there is no need to travel to a library to find the required book or books.
- Unless the required book can be found in a library, there is a need to buy it – information on the internet is usually free of charge.
- Pages on the internet can have multimedia elements (for example videos, animations, cartoons and music/voiceovers) that make learning more interesting and often make it easier to understand the topics – unless textbooks have accompanying CD-ROMs, this option is not available in books.

Disadvantages

- The internet is not regulated – anything can be posted on a web page and, consequently, information may be biased or totally incorrect (books, on the other hand, usually undergo some form of review before being published).
- There is always the risk of accessing inappropriate websites when using search engines; these can take many forms and can be very distressing to certain people.
- It is too easy to be distracted when searching on the internet – users can find computer games or enter social networking sites instead of doing their work.
- There is always the risk of 'information overload' if the user lacks the necessary experience or expertise when using search engines.
- Because it is very easy to copy material from the internet, there is a huge risk of plagiarism; this is more likely to occur than when using books since this requires considerably more effort than a simple copy and paste.
- Some research skills are lost when using the internet as search engines do all the work for you.

Why are internet searches to find relevant information not always fast?

When using search engines, there is always the danger of information overload. It is possible for millions of sites to be found matching the given criteria. Unless the user narrows down their search criteria, it can take a long time to find out exactly what they are looking for. Also, if the user is uncertain of what needs to be asked, it can also take a long time to obtain only relevant information.

While search engine companies deny it, certain websites are also placed at the top of their lists. When a user keys in certain words, these websites in the list always show up first in the search results and may not contain exactly what the user is looking for. Search engines also rank the time it takes to load up pages from websites – the fastest are given priority when the results appear on the screen. All of this means that the user may not find exactly what they are looking for when using the search engine.

The actual operation of search engines is very complex and is beyond the scope of this book.

Why isn't it always easy to find reliable information on the internet?

When using a search engine to find information on the internet, there is no guarantee that the material returned is accurate or unbiased. Essentially, anybody is able to set up a website and write whatever they like without it having to be first verified (the only stipulation is that the material posted doesn't break any laws – if it does, then the author is liable to criminal prosecution). However, the material can be inaccurate or unverified and it can also be biased towards one way of thinking only. Unlike books, the material posted on websites doesn't have to be checked by other people to ensure it is factually correct. It is also possible for search engines to suggest websites that are completely out of date so that the information displayed on the web pages is no longer correct or relevant. It is arguable whether or not policing of the internet would improve this situation – this was covered in some detail in Chapter 9.

How can you evaluate the reliability of information found on the internet?

- Anybody can set up a website (claiming to be factually accurate), so information is not necessarily reliable or accurate.
- Some commercial websites will be biased (to advertise their products, for example).
- If a website has excessive advertising it could be unreliable (due to pressures from those advertising on their website).
- If the advertising on a website is related only to its own products it could be unreliable (again due to arguments claiming that their products are the best to carry out a specific task).
- It is possible to use the final part of a URL to identify a website's reliability – for example, websites ending with: .ac and .gov are more likely to be reliable.
- If a comparison of information from reliable sites or reliable/authenticated student books is made, this will often help to show if the information is reliable.
- It is always a good idea to see if responsible bodies have endorsed the website.
- Check if the website has links to other reliable websites or to unreliable websites.
- If a website has testimonials, this can indicate reliability.
- If the date of the last update was a long time ago it is likely to be unreliable or out of date.

If the author of the website has good credentials, then it is more likely for the content to be reliable

Exercise 10a

Research a number of search engines and write down ways to narrow down searches using different symbols and key words (such as '+' and 'OR'). Take screenshots of your results to see how using these symbols and keywords narrows down the number of results shown.