



## **Contents**

---

<b>1 Introduction to T215 taster material</b>	<b>2</b>
<b>2 What T215 is like</b>	<b>2</b>
<b>3 What T215 is about</b>	<b>3</b>
<b>4 Assessment on T215</b>	<b>4</b>
<b>5 Study calendar</b>	<b>4</b>
<b>6 Extracts from the module</b>	<b>5</b>
<b>Extract 1</b>	<b>7</b>
<b>Extract 2</b>	<b>16</b>
<b>Extract 3</b>	<b>23</b>
<b>Extract 4</b>	<b>32</b>
<b>Extract 5</b>	<b>42</b>
<b>Extract 6</b>	<b>49</b>

# 1 Introduction to T215 taster material

This document has been designed to give you an idea of what it is like to study T215 Communication and information technologies. It contains extracts from Blocks 1, 2 and 4 and an example of an assessment question from Block 1. We hope that by browsing through the material you will get a feel for the level of the module, its general style and approach, some of the topics covered, and the time you are likely to need for studying.

We hope this taster material will be helpful to you but please remember...

- It's a very small sample of a large module and so can only give an approximate idea of level and content.
- The pack is intended to give a general overview, not to act as a preparatory pack. It should be read in conjunction with the T215 module information accessible via the Study at the OU website (Undergraduate ICT and Computing section) with a full module description at <http://www3.open.ac.uk/study/undergraduate/course/t215.htm>.
- The extracts selected have been chosen to give a good representation of a range of topics and approaches used. We have tried to select material which does not rely too heavily on what has gone before, but occasionally concepts may be used which were more fully explained earlier in the module.

Here is one suggestion for a way of using this document to give you a brief taste of being a T215 student.

- Read through Section 2 *What T215 is like* to get an overview of the module.
- Read through Section 3 *What T215 is about* to get an overview of the topics covered.
- Read through Section 4 *Assessment on T215* to get an overview of how the module is assessed.
- Have a look at Section 5 *Study schedule* and the descriptions of the extracts in Section 6 *Extracts from the module* to get an idea of how they fit into the module.
- Read through Section 6 *Extracts from the module* but don't get bogged down in the details.

## 2 What T215 is like

T215 Communication and information technologies is a level 2, 60 credit module spread over about 9 months, as shown on the Study calendar in Section 5. The module is structured into six blocks, each designed to occupy approximately five or six weeks of study.

The first five blocks are supported by study material, both printed and online, which consists of explanatory text mixed with examples, exercises and activities for you to complete. In Blocks 2 and 3 part of your study will involve you in working collaboratively with other students in a small group. In Blocks 3 and 5 you will need to install some third-party software on your computer and work with it.

In Block 6, the final block of the module, you will undertake a small project that will form the end-of-module assessment (EMA) discussed further in Section 4 *Assessment on T215*. No study material is supplied for this block.

Spread through the module is a number of assignments for you to complete at points indicated on the study calendar. These are described in more detail in Section 4 *Assessment on T215*.

### **3 What T215 is about**

Digital communication and information technologies have become fundamental to the operation of modern societies. New products and services are rapidly transforming our lives, both at work and at play. This module will help you to learn about these new developments and some of the issues arising from their use, and will equip you with the understanding and skills to continue learning about them in the future. You will study the core principles on which the new technologies are built and, through a range of online and offline activities, investigate new topics and technologies and develop a variety of skills.

The main technical topics covered in the module are:

- Digital data storage
- Wired and wireless local-area networks
- Service oriented architecture
- Mobile communication devices
- Mobile telephone systems
- The Global Positioning System (GPS)
- Online collaborative and social network technologies
- Privacy and surveillance
- Encryption
- Biometric identification
- Digital representation of sound and images.

The module has a strong focus on developing the skills of:

- Written communication (writing technological articles and reports)
- Critical evaluating and improving your own work
- Collaborative online working
- Information literacy (finding information online)

The module will also help you to develop your skills in the following:

- Numeracy
- Reading technological documents
- Making effective use of feedback
- Independent learning

During your study of the module you will engage in the following main practical tasks:

- Working in a group to create a wiki

Working in a group to create a simple web site

Creating a short video

## 4 Assessment on T215

There is a tutor-marked assignment (TMA) and a computer-marked assignment (CMA) at the end of each of Blocks 1 to 5 except for Block 3 which has only a TMA. CMAs and TMAs are submitted on-line at points indicated on the study calendar in Section 5.

Each CMA consists of about 10 multiple-choice questions. Each TMA consists of two to four questions, and for most TMAs one of the questions will ask you to write a document about an aspect of technology introduced in the block. Your answers to these types of questions will be marked on the accuracy and appropriateness of your technical content and the quality of your writing (which is developed through specially designed learning materials included in the module). Your tutor will score and comment on your answers to the TMA questions. There are likely to be plenty of comments from your tutor, as TMAs are used as a way of providing individualised teaching and encouragement for you.

There is no final examination on T215. Instead there is an end-of-module assessment (EMA). This occurs in Block 6 and consists of a short project in which you will find your own resources (for example, by using the Web) to investigate a specified topic or topics in communication and information technologies but not covered in the module materials, and write a report and other material based on what you have learned.

In order to pass T215, you need to achieve 40% or more on the EMA and an average of 40% or more on the TMAs and CMAs.

## 5 Study calendar

The Table 1 below shows the study calendar for the module. The start of study week 1 usually falls on either the last Saturday of January or the first Saturday of February.

**Table 1 T215 study calendar**

<b>Study week</b>	<b>Module text</b> <i>Note : Some components are provided online</i>	<b>Other components</b> <i>Note : This gives an indication of the relationship of components to the module texts, not exact dates</i>	<b>Assignments</b>
1	<b>Block 1 - Storing and sharing</b>	Module Guide	
2		Online: Cisco Academy	
3			
4			
5			CMA 41 TMA 01
6	<b>Block 2 - Exploring and enquiring</b>	Block 2 Document Book; start of some group collaboration	

7		
8		T215 DVD
9		
10		CMA 42 TMA 02
11	<b>Block 3 - Creating and collaborating</b>	Block 3 Reader; start of group work
12		WordPress Guidance
13		
14		
15		
16		TMA 03
17	<b>Block 4 - Protecting and prying</b>	Block 4 Document Book; T215 DVD
18		
19		
20		
21		
22		CMA 43 TMA 04
	<b>Study break week</b>	<b>(can be taken anytime up to TMA 05 cut-off)</b>
23	<b>Block 5 - Entertaining and explaining</b>	T215 DVD; Audacity software
24		Avisynth software
25		
26		
27		CMA 44 TMA 05
28	<b>Block 6 - Project</b>	
29		
30		
31		
32		

## 6 Extracts from the module

This section provides six extracts from T215. Extracts 1, 2 and 3 give some examples of the technical content of the module, Extract 4 gives an example of technological issues covered in the module, and Extract 5 gives an example of the module's skills development material. Each of these extracts is preceded with a brief indication of where in the module it occurs and how the ideas within it are developed later. Where an extract includes any self-assessment activities, the answer to these activities is given at the end of the extract and not, as the text indicates, at the end of the part.

Finally, Extract 6 gives an example of one type of TMA question you are likely to meet at the end of the first block of the module.

## Extract 1

*This extract is taken from Block 1 **Storing and sharing** and comes from Part 5 **Wi-Fi and wireless local area networks**. Other sections (not included) in this part describe how the wireless medium is shared between multiple users in a network and the theoretical data rates that can be achieved. Part 5 also includes sections on securing a wireless local area network and briefly introduces some other mobile wireless communication technologies, some of which are explored in more detail in Block 2 *Exploring and enquiring*.*

## Section 2: Wireless communication

This section offers a brief introduction to some of the general principles of wireless communication in order to help you to grasp what is to follow. You may well have met some of these principles in previous studies, in which case you can regard this section purely as revision. You will also be meeting some of the concepts again in Block 2, where they are discussed within the context of mobile phone technology.

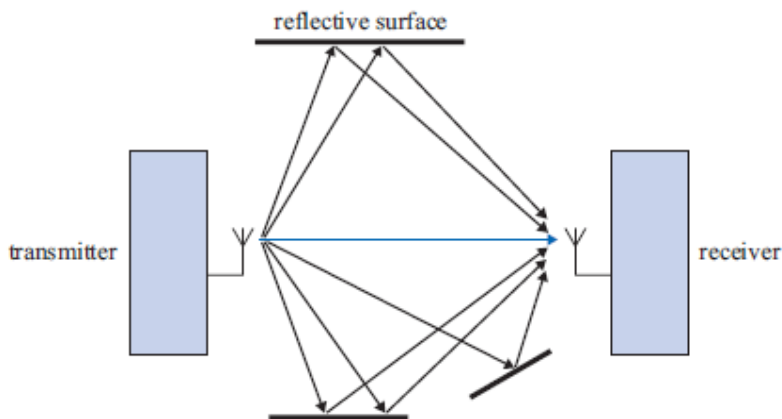
It is well over a century since Guglielmo Marconi demonstrated to an amazed London audience how a message could be transmitted wirelessly across a room. Marconi's message was a code produced by the simple on-off tapping of a telegraph key. The technology of wireless communication has developed significantly since then, allowing us to send and receive far more complex messages, but the basic principles of wireless communication using radio waves remain unchanged.

### 2.1 General principles of wireless communication

Radio waves are a particular group of electromagnetic waves, characterised by their frequency, which lies between about 3 Hz and 300 GHz. This band of frequencies is known as the [radio frequency spectrum](#) (often abbreviated to radio spectrum).

Radio waves occur naturally in the environment; for example, those caused by cosmic radiation. But, for communication purposes, radio waves are created using electronic circuitry and launched into the atmosphere via a radio transmitter. Radio waves created for the purposes of wireless communication are usually referred to as [radio signals](#). These signals can propagate from their source in all directions, becoming weaker (attenuated) the further they travel. If they are transmitted using different frequencies, many radio signals can exist in the same space at the same time without interfering with each other. Radio waves at the lower frequency end of the spectrum can propagate long distances with very little attenuation. These radio frequencies are used for purposes such as navigation and long-range broadcasting. The radio waves at the higher frequency end have a much reduced range and are absorbed more readily by physical objects such as walls. These higher frequencies are used for line-of-sight transmission between transmitter and receiver, such as microwave communication links. There are also differences in data carrying capacity: higher frequencies provide a faster data rate and so have the potential to carry more data per unit of time.

The frequency of a radio signal isn't the only factor that affects propagation distance. It is also influenced by the design of the equipment (this relates mostly to the transmission power and receiver sensitivity) and the propagation path. Radio signals can travel unhindered in an open space with few obstructions, but in enclosed areas, such as buildings, some objects will absorb radio signals (particularly those at the higher frequencies, as I've noted earlier) while others, such as metal filing cabinets and certain wall coverings, can act like mirrors and reflect radio signals, causing them to take multiple paths to the receiver, as illustrated in Figure 5.1.



**Figure 5.1** Radio signals travel over different paths due to reflection from walls

The overall effect of the multipath environment depends on the number of reflective surfaces, the distance from the transmitter to the receiver, the equipment design and the radio technologies used. Reflected signals reach the receiver at a slightly different time to the dominant line-of-sight signal (represented by the coloured arrow in Figure 5.1) and can act as interference, which attenuates (weakens) the signal. This is an effect known as [multipath fading](#).

I'll now describe, very briefly, how radio waves can be used to transmit messages. At the sending end, the message is superimposed upon a radio carrier wave (a process known as [modulation](#)), and is then extracted from the carrier wave ([demodulation](#)) at the receiving end. This is accomplished by electronic circuitry to modulate the carrier wave, a radio signal to transmit the modulated signal, a radio receiver to receive it and further electronic circuitry to demodulate it.

In modern wireless communication systems the carrier wave occupies a prescribed band of frequencies, often referred to as a [channel](#). One of the most significant developments in radio communication has been a process known as [multiplexing](#), which enables multiple data signals to be transmitted simultaneously over the same channel. You'll be learning more about modulation and multiplexing in Block 2 of this course.

## 2.2 Regulation

If the human eye could see all the radio signals passing through air we'd see a very crowded space indeed. Imagine being able to see the signals carrying the public radio and television broadcasts, the signals from mobile phone masts, road traffic information systems and remote control devices, to name but a few. Each type of signal occupies its own portion of

the radio frequency spectrum. If one kind of signal is being transmitted at a particular frequency, then that same frequency is not available to be used by another signal in the same way in the same vicinity.

The radio frequency spectrum, though large, is a finite resource and there are many competing users and uses vying for a portion. Furthermore, some radio frequencies are more suitable for particular purposes than others are. To ensure that the radio spectrum is used in the best way and that interference between signals is minimised, some form of regulation and allocation is required. At an international level this is done by the [International Telecommunications Union \(ITU\)](#), a United Nations body that has the power to allocate frequency bands for broad categories of use, such as public broadcasting, satellite communications and global positioning systems (GPSs). Amongst these designated bands are a range of frequencies, known as the [ISM frequencies](#), for unlicensed use originally by the industrial, scientific and medical (ISM) communities. I shall say more about these bands later.

Although the ITU has the responsibility for the broad allocation of frequency bands, the regulation, governance and licensing of these bands at a local level is the responsibility of individual countries. This is usually done by regulatory bodies that are appointed by governments. In the UK this is the Office of Communications (Ofcom) and in the USA it is the Federal Communications Commission (FCC).

## Section 3: Wireless LANs: Wi-Fi

Previous sections in this part have already established what a wireless LAN is. With very few exceptions, wireless LANs conform to a set of standards with the generic name of Wi-Fi (though you may also see it written as wifi, WiFi, Wi-fi and other variations on the theme). Because of this, wireless LANs are generally referred to as Wi-Fi networks.

I shall begin with an overview of Wi-Fi standards and then move on to describe key aspects of some of the technologies they define.

### 3.1 Wi-Fi standards

The standards that have become known as Wi-Fi standards are specified by the Institute of Electrical and Electronics Engineers (IEEE) and known as the IEEE 802.11 family of standards for wireless LANs. The term Wi-Fi is used interchangeably with IEEE 802.11 in the same way that the term Ethernet is used interchangeably with IEEE 802.3 (the IEEE family of standards that define wired LANs). In fact, there are many similarities between the 802.11 and 802.3 families of standards – for example, both of them are based on a layered architecture model. (An example of a layered architecture model is the Transmission Control Protocol/Internet Protocol (TCP/IP) model, which you met in Part 4.) These similarities aren't really surprising, since both standards are designed to perform a broadly similar task: that is, getting data across a network (albeit by different types of communication link).

## IEEE

The IEEE (pronounced eye-triple-e) describes itself as the world's leading professional association for the advancement of technology (IEEE, 2009). Amongst its many tasks, it develops and defines standards covering a wide range of industries, including telecommunications and information technology. It produces some 30% of the world's literature in the electrical and electronics engineering and computer science fields.

At the time of writing the IEEE provides access to almost 2 million documents online for its members or by subscription through a searchable database – IEEE Xplore. (Many of these documents are available to you as an Open University student, and can be accessed through the OU Library.)

The term Wi-Fi is actually a trademark of the Wi-Fi Alliance (see box) – an organisation set up in 1999 to promote the use of products which correctly implement the 802.11 standard.

As you learned earlier, transmission on most radio frequencies is strictly controlled by governments who license their use. There are, however, some bands of frequencies, known as the ISM bands, which are licence-free. Those of interest here are known as the 2.4 GHz band and the 5 GHz band (there are also other frequency bands designated for ISM use). These are the frequencies specified for wireless LAN use in the 802.11 standards. 2.4 GHz and 5 GHz are, of course, abbreviations, since the term 'band' implies a range of frequencies. What is known as the 2.4 GHz ISM band actually runs from 2.4 GHz to 2.4835 GHz, and the 5 GHz band runs from 5.15 GHz to 5.85 GHz. In the sections that follow, when I refer to the 2.4 GHz and 5 GHz bands I will be referring to their equivalent ISM frequency bands. It's important to appreciate that some governments don't allocate all of the frequencies in the ISM bands. Governments may also impose limits on maximum power output allowed when transmitting on some ISM frequencies.

## The Wi-Fi Alliance

The Wi-Fi Alliance describes itself as a global, non-profit industry association with over 300 companies as members (Wi-Fi Alliance, 2009a). It was formed to address the problem of incompatibility between products produced by different manufacturers, some of which did not fully implement 802.11, while others included proprietary extensions.

The Wi-Fi Alliance has a comprehensive testing and certification programme. Wi-Fi certified products are guaranteed to be interoperable.

The IEEE started development of the 802.11 standards for wireless LANs in the early 1990s, and development of different versions is ongoing. The main 802.11 standards and some brief details about them are given in Table 5.1. Where you see references to OFDM and DSSS, these relate to the type of multiplexing and modulation schemes used. OFDM stands for [orthogonal frequency division multiplexing](#) and DSSS stands for [direct sequence spread spectrum](#). The actual details of these schemes aren't of concern to us here, so I won't discuss them further, but you'll be meeting OFDM again in Block 2.

**Table 5.1 The main 802.11 standards**

Version	Date of ratification	Operating band	Modulation method	Maximum data rate	Notes
802.11a	1999	5 GHz	OFDM	54 Mbit/s	5 GHz band not available in Europe in 1999, so 802.11a is almost non-existent in the UK and other European countries
802.11b	1999	2.4 GHz	DSSS	11 Mbit/s	2.4 GHz band available in Europe in 1999 (and since), so 802.11b used in the UK
802.11g	2003	2.4 GHz	OFDM	54 Mbit/s	Developed to provide a data rate comparable to 802.11a for those locations where use of the 5 GHz band was not permitted. Is backwards compatible with 802.11b
802.11n	2009 (forecast at the time of writing)	2.4 GHz 5 GHz	OFDM OFDM	288 Mbit/s 600 Mbit/s	5 GHz band was released for unlicensed use in the UK in 2003

### Expressing data rates

It is usual to express data rates as the number of bits transmitted per second. This can be shown as bit/s or bps. For example, kbit/s or kbps indicates kilobits per second; Mbit/s or Mbps indicates megabits per second.

### Activity 5.6 (exploratory)

Table 5.1 shows that 802.11a achieves a data rate in the 5 GHz band that is almost five times that achieved by 802.11b in the 2.4 GHz band. Can you identify any possible factors for this?

#### Comment

One factor you may have identified is that 5 GHz is roughly twice the frequency of 2.4 GHz. As you saw in Section 2.1, higher frequencies are generally able to carry data at a faster rate than lower frequencies can. You may also have noticed that 802.11a uses a different modulation scheme to 802.11b.

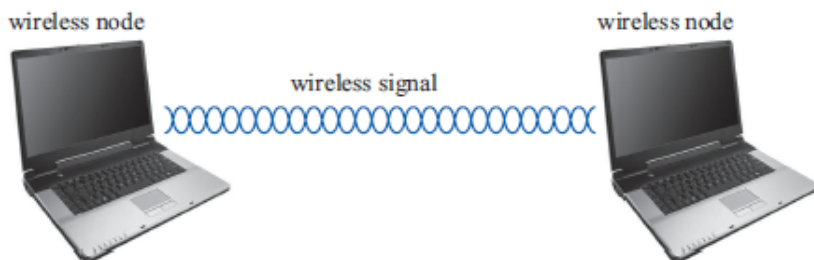
## 3.2 Wireless LAN configuration and equipment

End-user devices access a wireless network using small transmitter/receiver units. These are described as [wireless LAN adapters](#) or sometimes [wireless network interface cards \(wireless NICs\)](#) and are analogous to the [network adapter cards \(NICs\)](#) required to connect to a wired LAN. They provide the interface between the device and the network. Wireless LAN adapters are fully integrated in most notebook computers, as they are in many personal digital assistants (PDAs) and smartphones, but they are also available as PCI cards and USB devices, which are systems for computer connectivity. Desktop computers may have integrated systems, or an additional PCI card adapter can be fitted.

End-point devices in a wireless network are often referred to as [nodes](#) or [stations](#). (The latter term arises from their ability to transmit and receive

radio signals – hence being radio stations.) From here on, I shall refer to all the end-point devices in a wireless network as nodes.

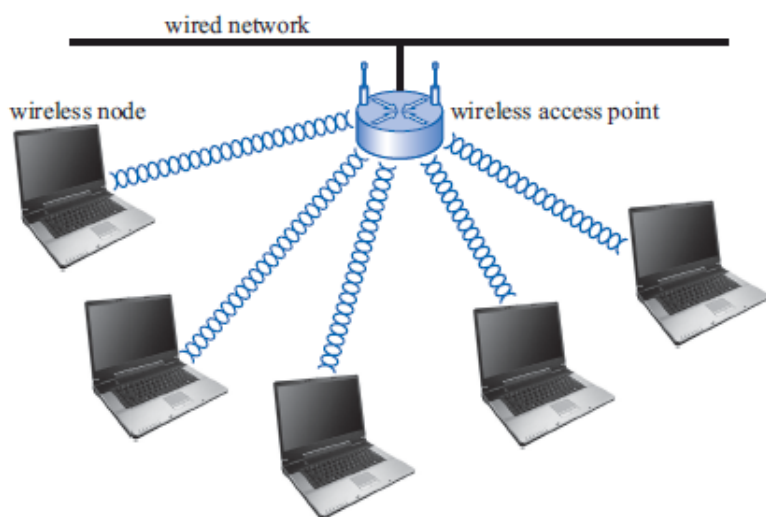
There are two basic configurations for a wireless network. The simplest is an independent network known as an **ad hoc** or **peer-to-peer network**. Each node in the network needs a wireless network adapter but no further equipment is needed. When two or more wireless nodes are within range, they can set up an ad hoc network. Figure 5.2 represents an ad hoc network that consists of just two nodes, though it is possible for ad hoc networks to contain multiple nodes.



**Figure 5.2 Representation of an ad hoc (peer-to-peer) wireless network of two nodes**

Ad hoc networks aren't used much and generally wouldn't be thought of as wireless LANs, but occasionally connecting to another person's notebook computer to swap files for example can be useful. An advantage of an ad hoc network is that usually it doesn't need any administration or preconfiguration.

The second basic wireless network configuration is one that is used as an extension to a wired network, and is usually situated within a building or a communal area such as a university campus. This type of configuration is known as an **infrastructure network**, represented in Figure 5.3.



**Figure 5.3 Representation of an infrastructure wireless network**

The main component of this type of network is a transmitter/receiver unit called an **access point (AP)** or sometimes a **wireless access point (WAP)**. The AP connects to a router, which in turn connects to a wired LAN or to a broadband connection. For small office and home networks it's common for the AP and the router to be housed together in a single unit, and in the

discussions that follow I shall assume this to be the case. Therefore, when I refer to the functions of the AP I shall also be including the routing functions.

The AP forms part of the wired network infrastructure and is not mobile. Its purpose is to receive, buffer (store for a short time) and transmit data between one wireless device and another or between a wireless device and the wired network. To perform these functions it also has to control wireless network traffic in the immediate area.

Any form of wireless communication is limited by how far the signals can travel. Wireless LANs in larger organisations may use several APs to cover a larger area, though APs within range of each other must be set to use different frequencies or channels (see Section 3.3) so that they don't interfere with each other.

A moving wireless node is associated with a single AP at any one time. AP areas overlap to allow continuous communication as the node is moving. The node will always try to communicate with the AP producing the strongest signal, so as the user moves close to the boundary of two or more APs there is a transition to the AP with the strongest signal. When I talk about wireless LANs in the following sections I shall be referring to infrastructure networks.

### 3.3 Transmission channels

802.11 specifies the 2.4 GHz band in terms of 14 channels, which are listed in Table 5.2 and identified in terms of their central frequency. For each channel, the difference between their highest and lowest frequency (this is their **bandwidth**) is also specified. In the 802.11b standard this is 22 MHz (0.022 GHz), and in the 802.11g standard, which uses a different, more efficient, modulation method, this is 20 MHz (0.020 GHz). In the discussion that follows I will describe the 20 MHz bandwidth channel, as this provides slightly easier figures to work with.

With a 20 MHz bandwidth, this means that each channel occupies a band of frequencies lying from 10 MHz (0.01 GHz) below to 10 MHz above its central frequency. For example, channel 1 occupies the band of frequencies lying between 2.402 and 2.422 GHz.

**Table 5.2 Wi-Fi frequency channels in the 2.4 GHz range**

Channel ID	Frequency (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462
12	2.467
13	2.472
14	2.484

### Activity 5.7 (self-assessment)

Looking at Table 5.2, what is the band of frequencies occupied by

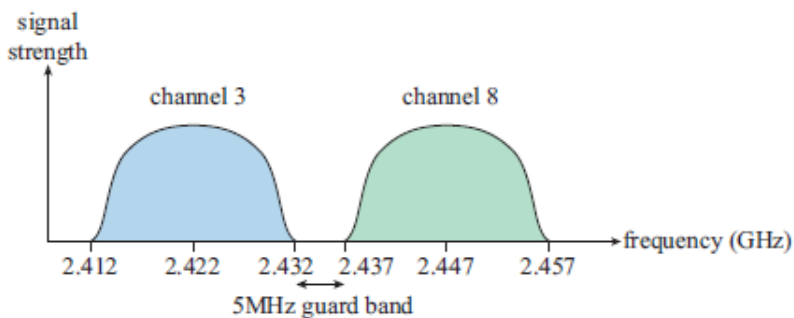
- (a) channel 3
- (b) channel 5?

What problem would arise if one Wi-Fi network transmitting on channel 3 was within range of another Wi-Fi network transmitting on channel 5?

#### Comment

The answer is at the end of this part of the block.

From the answer to Activity 5.7, it is clear that even in situations where all 14 channels are available for use, it is not possible to transmit signals simultaneously in the same vicinity on all channels. In fact, the 802.11b and g standards specify a 25 MHz separation between centre frequencies of co-located channels. (In this context the term **co-located** means being within radio range of each other.) This provides a 5 MHz frequency gap known as a **guard band** to prevent interference. Figure 5.4 illustrates the 5 MHz guard band lying between the frequency bands of channel 3 and channel 8.



**Figure 5.4** A 5 MHz guard band lying between the frequency bands of channel 3 and channel 8

Different countries allocate the channels in different ways. For example, in the UK only channels 1 to 13 are available and in the USA only channels 1 to 11, whereas Japan uses 1 to 14, France uses 10 to 13 and Mexico is limited to channel 11 only.

Channel 11 tends to be the default for home systems, though this can easily be changed if a nearby network is operating on the same channel.

### Activity 5.8 (self-assessment)

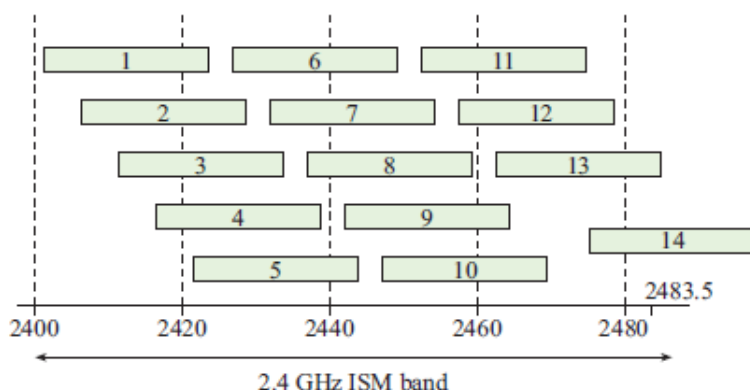
While setting up a wireless 802.11g wireless network (in the UK) you note that another nearby network AP is set to use channel 11.

- (a) Which of the other channels would be the best choice for your new network?
- (b) What is the maximum number of non-overlapping channels available in the UK? (Reminder: the 2.4 GHz ISM band runs from 2.4 to 2.4835 GHz.)

#### Comment

The answer is at the end of this part of the block.

You will have seen from the answer to Activity 5.8(b) that the maximum number of collocated channels in the 2.4 GHz band is three. This can be seen more clearly in Figure 5.5.



**Figure 5.5 Channel overlap for 802.11 in the 2.4 GHz ISM band**

The method of channel allocation in the 5 GHz band is broadly similar to that described for the 2.4 GHz band, but the much wider frequency spectrum of the 5 GHz band results in a much greater number of non-overlapping channels – up to a maximum of 24. Again, it's important to note that the actual number of non-overlapping channels available will depend on a country's regulatory policy. At the time of writing there are two 5 GHz frequency ranges permitted for licence-free use in the UK:

- Band A (5.150–5.350 GHz) provides eight non-overlapping channels
- Band B (5.470–5.725 GHz) provides 11 non-overlapping channels.

## Answers to self-assessment activities in Extract 1

### Activity 5.7

- (a) Channel 3 occupies the band of frequencies from 2.412 to 2.432 GHz.  
 (b) Channel 5 occupies the band of frequencies from 2.422 to 2.442 GHz.

Some of the frequencies used by channel 3 are also used by channel 5. This means that if these channels are used within range of each other the signals would interfere.

### Activity 5.8

- (a) The frequencies used in channel 11 lie from 2.452 to 2.472 GHz, so any channel that uses these frequencies cannot be used. This eliminates channels 12, 13 and 14 (though, of course, channel 14 is not available in the UK anyway). Also, there must be a 5 MHz guard band between channels, so only those channels that use frequencies below 2.447 GHz could be used. Channels 1 to 6 satisfy the required conditions.
- (b) The 2.4 GHz ISM band has a bandwidth of 83.5 MHz (0.0835 GHz). This is sufficient to accommodate no more than three separate channels with centres separated by 25 MHz.

## Extract 2

*Extract 2 is taken from Block 2 Exploring and enquiring Part 3 The technology of mobile telephone systems. Earlier sections of Part 3 have explained the evolution of mobile telephone systems from the original analogue system, known as first generation, to the GSM digital system known as second generation. The extract given here describes enhancements made to improve the performance of the GSM system. Later sections introduce a third generation mobile phone system (the universal mobile telecommunications system) and then look beyond it.*

## Section 4 Upgrades to GSM: 2.5G

Before you start to study this section it's important for you to remind yourself of the difference between a circuit-switched network, such as a telephone network, and a packet-switched network, such as the internet. You met these two types of network in the Cisco material you studied in Block 1, Part 4, in particular in Cisco's Section 1.4.2.

### Activity 3.11 (self-assessment)

What is the essential difference between a circuit-switched network, such as a telephone network, and a packet-switched network, such as the internet?

#### Comment

The answer is at the end of this part of the block.

### 4.1 GPRS: general packet radio service

Like the public switched telephone network (PSTN) and the 1G analogue telephone system, GSM was designed as a circuit-switched system. This was appropriate for voice calls, and also acceptable for the sort of short text messages sent via SMS. But the limitations of a circuit-switched system quickly became apparent when an attempt was made to offer a more sophisticated data transfer service, including web browsing, via GSM. Users found this service too slow – the maximum data rate in the 900 MHz band was 9.6 kbit/s and in the 1800 MHz band was 14.4 kbit/s. And for the service providers, it was an inefficient use of the time slots; a pair of slots (one for the uplink and one for the downlink) had to be dedicated to a particular user, yet there were only occasional transfers of data (the term 'bursty' is often used to describe this sort of sporadic yet intense data transfer). The solution to this problem was to provide an upgrade to GSM whereby a parallel network was provided to handle data transfers. That upgrade is known as general packet radio service (GPRS), which is packet-switched.

When a GSM network has been upgraded to GPRS, as it was by the UK's 2G providers during the early 2000s, voice traffic continues to be handled by mobile switching centres but there is a new network of GPRS service nodes (GSNs) to handle data traffic. Each base station is connected to both a mobile switching centre and a GSN; and as with mobile switching centres, a single GSN will probably control data traffic in several cells.

Just as mobile switching centres pass some voice calls directly between themselves but pass others into the PSTN, so GSNs pass some data traffic

directly between themselves and pass other data traffic out into other data networks, the internet for example.

In order to be able to make use of GPRS services, users need a suitably equipped mobile terminal. This terminal will register with both the voice network and the data network. The most usual arrangement is that the user can have both voice and data switched on but can use only one of them at any given time. A mobile terminal with this behaviour is offering 'class B GPRS'. Class A GPRS would enable both voice and data to be used simultaneously; class C GPRS would require the user to switch manually between voice and data as required. The majority of mobile terminals on the market offer class B GPRS.

When a mobile terminal passes from one cell to another while transmitting or receiving data, a handover process akin to that used for voice calls is required.

Whereas voice calls are charged on the basis of time, data transfers are often charged on the basis of the quantity of data transferred. Therefore the mobile terminal can be left connected into the data network for a long time without necessarily incurring high charges. This 'always on' facility is useful for data transfers, as it means that data transfers can be made without the short but noticeable delay that voice calls incur while they are being set up.

All this is very well, but between the mobile terminal and the base station frames are still transmitted at the carrier frequencies allocated to that cell, and frames are still made up of eight individual time slots. How can data use these time slots and frames to achieve higher data rates?

The answer is that time slots are allocated differently in GPRS from GSM. They are allocated on a needs basis, rather than on the basis of being fixed for the duration of the call. So any time slots not currently being used for voice calls can be used for packets of data, and more than one time slot per TDMA frame can be allocated to a single user. This is known as [multislot operation](#). If there is little voice traffic in a cell, then more resources can be allocated to data transfers and more data is transferred per second. But if there is a great deal of voice traffic, then much less data will be transferred. This is an efficient use of the network resources, though it does mean that the users who are accessing data will experience fluctuating data transfer rates.

As well as multislot operation, GPRS can achieve higher data rates through adjusting the amount of error correction being used. This means that the GPRS time slots are, in some circumstances, able to use a higher proportion of the bits in a time slot for user data than can GSM, which in turn leads to a higher data rate for users than can be achieved by GSM. However, the amount of error correction needed depends on how far the mobile terminal is from the base station (in general, a weaker signal will lead to more errors in the receiver and so more error correction) as well as on how much interference there is. With a good clear signal near a base station, a maximum data rate of 21.4 kbit/s per time slot can be achieved. At some distance from the base station, or with heavy interference, the rate may drop as low as 9.05 kbit/s per time slot.

### **Activity 3.12 (exploratory)**

If the maximum data rate of GPRS is 21.4 kbit/s per time slot, what do you think the maximum achievable data rate will be with GPRS, given

that all eight time slots in a time frame can, in certain circumstances, be allocated to the data transfer?

### Comment

You have probably decided that the maximum possible data rate will be eight times as much, namely 171.2 kbit/s, and this is correct. This will, of course, only be achievable in ideal reception conditions. What's more, there may be data to be transferred from several users simultaneously. If this is the case, these users will have to share the maximum possible data rate, so an individual user will experience a lower data rate. It would be more usual for an individual user to be allocated no more than two or perhaps three time slots per TDMA frame, leading to a maximum data rate per user of no more than 42.8 kbit/s or 64.2 kbit/s respectively – even in ideal reception conditions.

There is a level of service in the GPRS system that allows a single user to 'grab' all eight time slots in a frame, but this is both expensive and uncommon.

You should recall from Block 1, Part 5 that maximum data rates are not the same as throughput, in that management and control traffic will use up a proportion of the maximum available data rate. Actual throughput in GPRS networks will, therefore, be less than the values mentioned in the comment to Activity 3.12.

As GPRS is an enhancement to GSM, a 2G system, GPRS is sometimes referred to as a '2.5G' system. It's important to appreciate that this is simply a convenient way of describing this system. It is not a term with an 'official status', as are 2G and 3G.

## 4.2 EDGE: Enhanced Data rates for GSM Evolution

Although the maximum data rates that can be achieved in the GPRS system are an improvement on those achieved in plain GSM, they are still well below the rates that can be achieved by desktop computers connected to the internet, or even by notebook computers using Wi-Fi. **EDGE**, which stands for Enhanced Data rates for GSM Evolution, is a step beyond GPRS in the data rates that can be achieved.

In the long term, 3G is the solution to the need for higher data rates (see Section 5), and indeed in the UK, where 3G services began relatively early and are relatively widely available, there is little provision of EDGE by the mobile telephone companies. But in those countries where 3G is less widely available, EDGE is deployed to a greater extent.

EDGE can achieve approximately three times the maximum data rate of GPRS, while still using the same infrastructure as GSM and GPRS. Indeed, the GSM Association claims that 'For many existing GSM/GPRS networks, EDGE is a simple software-upgrade' (GSM Association, 2008). This 'simple software upgrade' is, in fact, a complete change of the modulation technique used to superimpose the data on to the carrier prior to transmission to or from the mobile terminals, and a corresponding change to the demodulation technique used at the receiving end. Whereas plain GSM used a type of digital frequency modulation, EDGE uses a very different sort of digital modulation called 'phase modulation', specifically a version called 8PSK. This technique is described in the box 'Phase

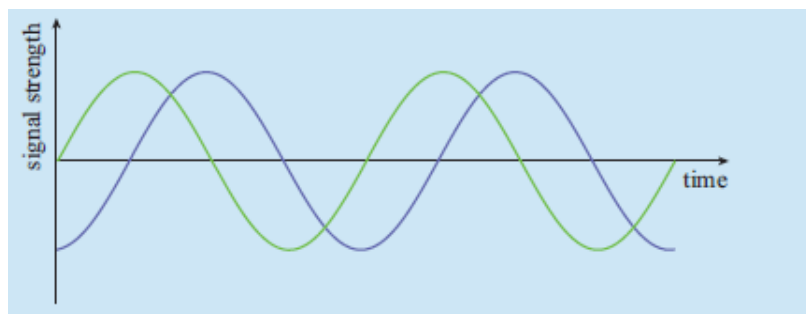
modulation'. The fact that 8PSK produces one of eight different phase levels, or symbols, for each possible group of three bits explains how EDGE can triple the maximum data transmission rate. It's important to appreciate, however, that this increased data rate has come at the expense of more processing of the signals.

In EDGE, speech signals and data packets are still multiplexed into time slots in frames, but now the components of the frames are being modulated using 8PSK. Therefore, not only is the maximum data rate for data transmissions tripled, but so is the transmission rate for speech signals. As this higher rate is not needed for individual voice calls, it can be used to accommodate more users simultaneously, and hence more users per cell.

As the mobile terminal has to deal with the signals sent by the base station and send suitable signals back, the mobile terminals used in an EDGE network also need to be equipped with appropriate software and circuits powerful enough to run that software. In fact, enhancements like EDGE are only really possible because the more powerful processing circuitry that is needed to run such software has become available at an affordable price.

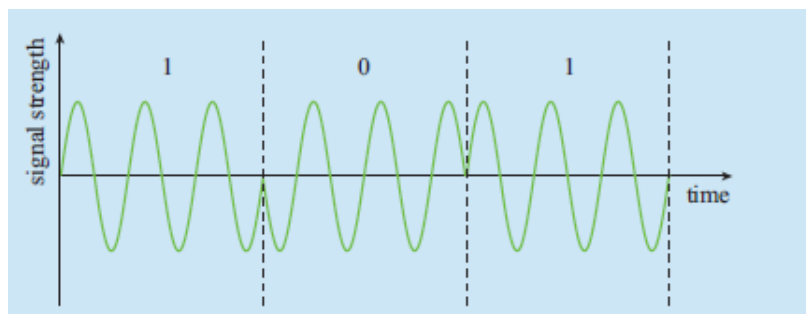
### Phase modulation

Figure 3.B3 shows two identical sinewaves. One of them is shifted in time with respect to the other – by one quarter of a full cycle. There is said to be a **phase difference** between them.



**Figure 3.B3 The two sinewaves have a phase difference of a quarter of a cycle**

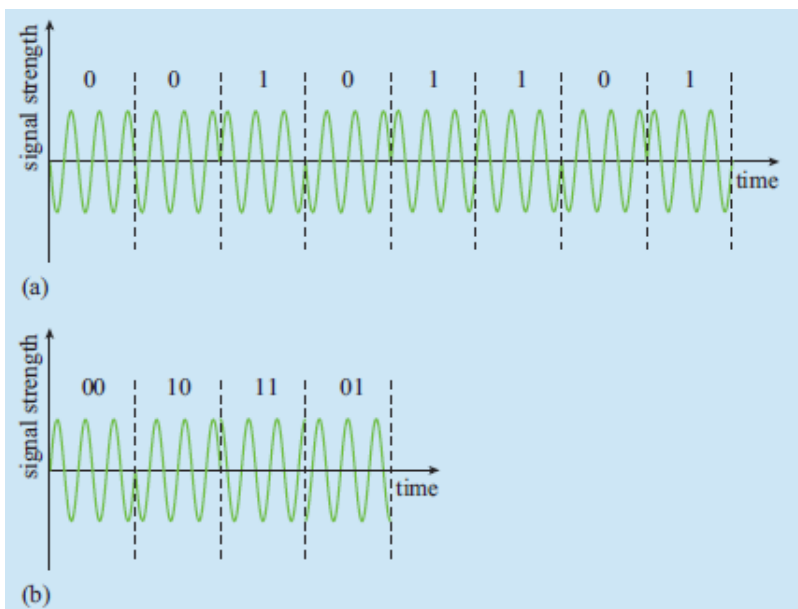
Differences in phase can be used in the transmission of binary data, using a process called **phase modulation**. Figure 3.B4 shows one way of doing so. You can see that the portion of the sinewave used to represent a 0 is 'upside down' with respect to that used to represent a 1. (This is equivalent to a phase shift of half a cycle.)



**Figure 3.B4 A phase-modulated binary signal**

The term **phase shift keying (PSK)** is often used to describe the phase modulation of a digital signal.

A significant feature of PSK is that the sinewaves don't have to be half a cycle apart in phase. They could be a quarter cycle or three quarters of a cycle for example. This raises an interesting question. What would happen if all four possibilities were used: no phase shift, a quarter-cycle phase shift, a half-cycle phase shift and a three-quarter-cycle phase shift? The answer is that it would be possible to use these four phase shifts to represent *pairs* of bits. So, for example, no phase shift could represent 00, a quarter-cycle phase shift could represent 01, a half-cycle phase shift could represent 10 and a three-quarter-cycle phase shift could represent 11. Such a scheme is called **quadrature PSK (QPSK)**, or sometimes quaternary PSK. Figure 3.B5 shows how the binary sequence 0010 1101 would be transmitted using (a) plain PSK and (b) QPSK. The important thing to notice is that *the same number of bits is transmitted in half the time in QPSK*, or, to put it another way, *QPSK doubles the data rate as compared with PSK*.



**Figure 3.B5 The binary sequence 0010 1101 transmitted using (a) PSK and (b) QPSK**

In a situation like the one in Figure 3.B5(b), where a particular phase shift represents a pair of bits rather than a single bit, it is usual to talk about **symbols** being transmitted and to quote a **symbol rate**. The bit rate can be calculated from the symbol rate when the number of bits per symbol is known.

Note that the four different phase shifts in QSPK form a digital system that is *not* binary: the number of states is limited (to four) but is not equal to two.

Another version of PSK uses eight different phase shifts, each an eighth of a cycle apart. This is called **8PSK**. Each of the eight different phase shifts can represent one of the eight possible patterns of *three* bits.

Similarly, 16PSK uses 16 different phase shifts and can represent all the possible patterns of four bits. In general  $2^n$  different phase

shifts can represent all the possible patterns of  $n$  bits, where  $n$  can be 2, 3, 4 and so on up to a maximum of 8 (beyond which value the phase shifts are so small that the error rate in detecting them becomes unacceptably high).

### Activity 3.13 (self-assessment)

If EDGE can achieve approximately three times the data rate of GPRS, what is the approximate value of the maximum data rate per time slot achievable with EDGE? Under what conditions will this maximum rate be achievable?

#### Comment

The answer is at the end of this part of the block.

Like GPRS, EDGE is sometimes described as a 2.5G system. But because it can achieve higher data rates than GPRS, it is sometimes alternatively described as a '2.75G' system.

## 4.3 Conclusion

In reading about upgrades to GSM, all of which are designed to make the system more attractive to current and potential users, it's important to remember that not all users want or need the enhanced facilities. There are plenty of users who are quite happy with plain GSM phones and would not want to spend money on a fancy phone with GPRS or EDGE facilities. They may well be pleased that the underlying GSM network has continued to function unchanged over many years, meaning that their phone has continued to work as before. Equally, there are users who impatiently await each upgrade and buy a phone with new facilities soon after it becomes available so they can use all the new features of the network.

In other words, there is what is called 'market segmentation' in the mobile phone market, and this is something that designers of upgrades need to be very aware of. It is one reason why 2G systems have continued to exist for so long, and may well continue to do so for some time yet, alongside the newer 3G systems.

One final point. The mobile telephone network is no longer the only way of accessing data on the internet while out and about: a few years ago some mobile terminals began to be equipped with Wi-Fi. These phones can therefore make use of Wi-Fi 'hotspots' as an alternative to the mobile telephone network.

### Activity 3.14 (exploratory)

What has changed in the move from 2G (GSM) to 2.5 systems? What has stayed the same? Can you suggest reasons?

#### Comment

The most obvious change is that the GSM system has been upgraded to deal with data transfers more effectively, forming a system known as GPRS. This has meant that GSNs (GPRS service nodes) and associated infrastructure have been added to the GSM network. It has also meant that the frames that are transmitted between base stations and mobile

terminals incorporate both time slots carrying voice calls and time slots carrying data transfers, with flexible sharing allowed.

A further upgrade, EDGE, has used a different modulation scheme to increase data rates still further.

In addition, mobile terminals that can handle GPRS and, where available, EDGE have had to be designed and manufactured.

The basic infrastructure of GSM has stayed the same – the cells, the mobile

switching units and so on. In addition, TDMA has continued to be used.

The changes have occurred because of the perceived need for more effective data transfer via the mobile telephone system. (Or maybe, to be a

little more cynical, because the mobile service providers hoped to increase their revenue by offering more services and the mobile phone manufacturers hoped to increase their revenue by offering higher performance phones.) The upgrades did, however, need to be effected as economically as possible, and with minimum disruption. The continued use of the original GSM network and of TDMA helped to achieve this.

## Answers to self-assessment activities in Extract 2

### Activity 3.11

In a circuit-switched network, such as a telephone network, a circuit is set up between the sender and the recipient and is maintained for the duration of the phone call, even if no one is speaking. The circuit cannot be used for any other call during this time. In a packet-switched network, such as the internet, a message is split up into packets which are sent one after the other from the sender to the recipient. Although the path taken by the packets can be the same for all packets, it does not have to be. In addition, packets from other messages can use the path whenever the original message has no packets to send.

### Activity 3.13

The maximum data rate per time slot will be approximately  $3 \times 21.4 \text{ kbit/s}$ , about  $60 \text{ kbit/s}$ . This will be achieved close to a base station in good reception conditions.

## Extract 3

*Extract 3 is taken from Block 4 **Protecting and prying** Part 5 **Encryption** which looks at the role of data encryption in preventing unauthorised people from having access to private information. The extract given here explains basic concepts of encryption. Later sections look at the vulnerabilities of some of the simple encryption systems, and methods for making them stronger. The building blocks of modern encryption systems are then introduced and some of the structures needed to support these systems.*

## Section 2 Encryption: basic concepts

I've already defined encryption as a process by which information is changed in some systematic way so as to hide its content from everyone except its intended recipient. The branch of science concerned with this concealment of information is known as **cryptology**, a word that has its roots in Greek from *kryptos* (hidden) and *logos* (word). Cryptology is the study of codes and ciphers, and divides into two branches: **cryptography**, the science of creating codes and ciphers, and **cryptanalysis**, the science of breaking them.

Cryptographers make a distinction between the terms 'codes' and 'ciphers', though in practice the two are often used interchangeably. In its pure sense, a **code** replaces whole words, phrases or groups of symbols with alternatives (or code words). The purpose of creating a code is not always for secrecy. Often a code is used simply as an abbreviation – such as the well-known 404 error message (see box) – or used to provide an alternative way of communicating information. Two examples are ASCII and Morse code.

- ASCII (American Standard Code for Information Interchange). This is used when storing and transmitting data, and uses only two different coding symbols (usually referred to as 1 and 0).
- Morse code. This is a standard for substituting groups of long and short pulses (or groups of dots and dashes) for letters. It has been used extensively in telegraphy because of its resistance to corruption from other signals during transmission, and because of its efficiency.

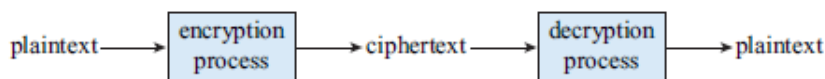
A code is the output of an encoding process (the reverse is decoding) and generally relies on sets of look-up tables (codebooks) for the conversion processes. When used for secrecy, the code becomes useless if the look-up tables fall into the wrong hands.

### 404 error message

There are a number of coded error messages a server can return to a client. '404 File not found' is one of these (and you may have seen it yourself when using your browser to find information on the Web). '404 File not found' means that the server was unable to locate the requested file.

A **cipher**, on the other hand, is the output of an operation that either replaces data symbols with alternative symbols, or rearranges existing symbols. In both cases the operation is done in a systematic way, following some set rules. A cipher is almost always created for reasons of

secrecy. **Encryption** is the process of transforming data (known as **plaintext**) into a cipher (known as **ciphertext**). **Decryption** reverses the process by transforming ciphertext back into plaintext. Figure 5.1 gives a simple graphical representation of these concepts.



**Figure 5.1 Encryption and decryption processes**

There are two basic methods for creating a cipher. One is to take a symbol (or a group of symbols) in the plaintext and manipulate it in a systematic way to produce a different symbol (or group of symbols), which becomes the ciphertext. The substituted symbols in the ciphertext appear in exactly the same order as the original versions in the plaintext. A cipher created using this approach is known as a **substitution cipher**.

The second method is to ‘scramble’ the order of the symbols in some systematic way. Using this approach, the symbols remain unchanged between plaintext and ciphertext, but the ordering of those symbols changes. A cipher created using this approach is known as a **transposition cipher**. In effect, the ciphertext is an anagram of the plaintext.

## 2.1 A simple substitution cipher: the Caesar cipher

One of the earliest recorded and best known ciphers was used by Julius Caesar in the 1st century BC and has since become known as the Caesar cipher. This is also one of the simplest of substitution ciphers, and as such it provides a good example for demonstrating some basic cryptographic concepts. It is unlikely that you will find any simple tutorial on cryptography without an explanation of the Caesar cipher, and this part of Block 4 is no exception!

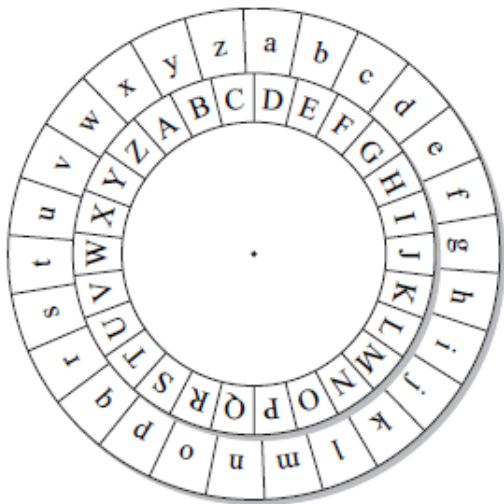
One of the methods Caesar used to preserve the confidentiality of a message was to substitute each letter in his message with the letter three places further forward in the alphabet. (This is an example of the systematic manipulation I referred to earlier.) Thus the letter ‘a’ would be substituted by the letter ‘d’, the letter ‘b’ by the letter ‘e’, and so on. To give an example using this method, the word ‘acme’ becomes DFPH. But what if I wanted to encrypt the word ‘zenith’ using the Caesar cipher? This presents something of a problem since the letter ‘z’ is the final letter of the alphabet. The solution is to jump back to the letter ‘a’ and continue the count as if the letters of the alphabet were arranged in a circle. ‘Zenith’ then becomes CHQLWK.

### Study note

*When giving examples of encryption, a convention often used is to show plaintext in lower case and ciphertext in upper case.*

When Augustus Caesar succeeded Julius Caesar, he changed the shift from 3 to 2, producing different ciphertext from a given plaintext. Indeed the choice of the shift is arbitrary; any shift of 1 to 25 would work equally as well, though of course the intended recipient for the encrypted text would need to know the choice in order to carry out the decryption process.

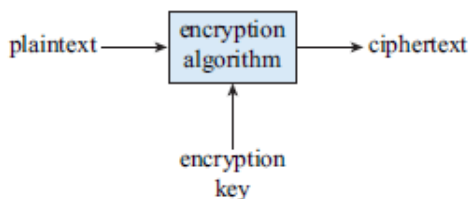
The circular nature of the Caesar cipher can be exploited to produce a simple encryption tool known as a cipher wheel, illustrated in Figure 5.2. The wheel is made up of two discs, one slightly smaller than the other. The alphabet is written around the circumference of both discs and the discs are fitted together at their centres in such a way that one can be rotated relative to the other, so any letter on the outer wheel can be aligned with any letter on the inner wheel.



**Figure 5.2 A cipher wheel**

Both the sender and the recipient need their own cipher wheel. The starting point for its use is with the wheels set so that each letter on the outer wheel is aligned with the corresponding letter on the inner wheel. The sender and recipient first agree on the number of shifts. Let’s say they have agreed to use a shift of three places forward as favoured by Julius Caesar. In this case the sender displaces the outer wheel by three places in a clockwise direction so that the ‘a’ on the outer wheel lines up with the ‘D’ on the inner wheel. This is then used to convert each letter in the plaintext message from the outer wheel to its partner on the inner wheel to form the ciphertext. To decipher the message the recipient also displaces the outer wheel clockwise by the same number of places, then converts the ciphertext letter on the inner wheel to its equivalent on the outer wheel to recover the plaintext.

When an encryption method can be carried out systematically by following some sort of set pattern or procedure, such a procedure is known as an **algorithm**. When the algorithm includes a variable that can be altered to produce a different outcome, the variable is called a **key**. So here we can say that Julius Caesar used a key of 3 and Augustus Caesar a key of 2. Figure 5.3 gives a graphical representation of the use of the encryption algorithm and the encryption key in the encryption process.



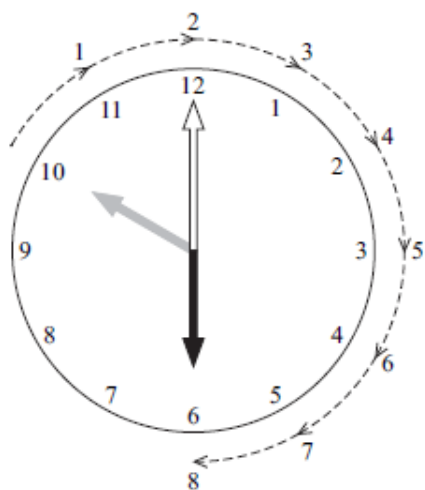
**Figure 5.3 Encryption process showing algorithm and key**

## 2.2 Mathematical representation

Modern communication systems use computers to process messages and, as you know, computers don't work with letters but with numbers. In this section I shall show how the Caesar cipher can be represented as a numerical algorithm that can be processed by a computer, but first I'll need to introduce you to modular arithmetic.

To do this I'll start by looking more closely at the Caesar cipher. As you've seen already, sometimes the shift will extend beyond the last letter of the alphabet, 'z', and when this happens the count continues to the first letter 'a'. It's as though the letters of the alphabet are arranged in a circle – as they are on each disc of the cipher wheel of Figure 5.2. Another way of looking at this is that the alphabet on each disc is arranged rather like the numbers on a clock face but using letters instead. In fact, if we were to represent each letter of the alphabet as a number, it would look a little like a clock with 26 different numbers rather than the 12 we're used to. We could think of the hour hand of the clock acting like the shift counter as it rotates clockwise. If the shift extends past the highest number on the clock face, the count simply continues round.

This analogy with a clock face provides us with a new way to think about addition. Here's an example that illustrates this. At ten o'clock this morning, my aunt phoned me to say she was returning home from her holiday and would arrive at the local train station in eight hours. She asked if I could pick her up on my way home from work. Using the 12-hour clock, what time would I need to be there? If I simply add eight to ten the result is 18 – a number that isn't present on the 12-hour clock. Instead, using the clock face representation (shown in Figure 5.4) I can use the hour hand as a shift counter, rotate it forward by eight places, and read off the result: six o'clock.



**Figure 5.4 Using the clock face representation to calculate elapsed time**

This simple example represents the process that is used in a branch of mathematics known as [modular arithmetic](#). Modular arithmetic operates with a limited set of [integers](#) (integers are all the positive and negative whole numbers, including zero). The number of integers in the set is known as the [modulus](#). Using the clock example, with a conventional

12-hour clock the modulus is 12; for a 24-hour clock, the modulus would be 24; in our alphabet example for the Caesar cipher, the modulus is 26.

Modular arithmetic provides us with a method for operating mathematically with a limited set of integers. Whatever mathematical operation we perform on these integers, the result must always be less than the modulus. As you saw from the 12-hour clock example, the result of moving forward eight hours from ten o'clock is six o'clock and not 18 o'clock. You observed a similar effect with the Caesar cipher when the shift took us beyond the letter 'z'. The Caesar cipher and the clock are examples of modular arithmetic in action.

Now, you are probably asking yourself what would have happened if my aunt was due to arrive at the station in two hours rather than in eight hours. Adding two to ten would give the result 12 – a number that is included on the 12-hour clock. It seems we have already broken one of the rules of modular arithmetic: that the result of any calculation must always be less than the modulus. But ask yourself this: what is the difference between 12 o'clock and zero o'clock? In fact, there is no difference at all in terms of the position on the clock face: 12 o'clock is simply a naming convention we have chosen. The actual position of the hour hand is at the very start of the rotation: in other words, at the zero position.

Fortunately, there is a more convenient way of arriving at the answers to calculations in modular arithmetic than using a clock face-type simulation. Before I explain this, I need to introduce some of the mathematical language used to describe the operations performed in modular arithmetic.

Returning to my earlier example of moving forward eight hours from ten o'clock using the 12-hour clock, mathematicians have a special way of expressing a calculation like this by saying that  $10 + 8$  modulus 12 is **congruent** to 6 modulus 12. In other words, 6 modulus 12 can be used in place of  $10 + 8$  modulus 12. Symbolically we would write this as

$$10 + 8 \text{ mod } 12 \equiv 6 \text{ mod } 12$$

but it's more usual to omit the first mod 12 so that it becomes

$$10 + 8 \equiv 6 \text{ mod } 12$$

Note that the congruence is represented by the symbol  $\equiv$  (the equivalence symbol). It's like an equal symbol with an additional bar.

Now I'll examine the process of how we can arrive at the answer to  $10 + 8$  mod 12 without using the clock simulation.

First add the two left-hand integers together in the conventional way:

$$10 + 8 = 18$$

If the result is equal to or greater than the modulus, subtract the modulus from the result, repeating the subtraction as necessary until the result is less than the modulus. In my example:

$$18 - 12 = 6$$

Now express the answer as a congruence modulus 12:

$$10 + 8 \equiv 6 \text{ mod } 12$$

Now I'll apply the same method to calculations for encryption using the Caesar cipher. First I need to convert the letters of the alphabet to numbers so that I can operate on them mathematically. I'll convert 'a' to 0,

'b' to 1, 'c' to 2 right through to 'z' to 25 as shown in Figure 5.5. You may wonder why I've chosen to set 'a' to 0 rather than to 1. This is because, as you saw above, the result of any calculation in modular arithmetic must always be less than the modulus. So if I'd set 'a' to 1 and therefore 'z' to 26, 26 would be an invalid result.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

**Figure 5.5 Numerical coding scheme for the Caesar cipher**

Using my chosen encoding, to encrypt the letter 'z' with a Caesar cipher using a key (shift) of 3 would give:

$$25 + 3 \equiv 2 \pmod{26}$$

The letter 'c' is represented by the number 2, so 'z' encrypts to C.

### Activity 5.1 (self-assessment)

Write out the following using mathematical notation and evaluate the result. Use the grid in Figure 5.5 to translate between alphabetic symbols and numerical values.

- (a) The ciphertext resulting from encrypting the letter 'f' using the Caesar cipher with a key of 6.
- (b) The ciphertext resulting from encrypting the letter 's' using the Caesar cipher with a key of 12.
- (c) The ciphertext resulting from encrypting the letter 'm' using the Caesar cipher with a key of 20.

### Comment

The answers are at the end of this part of the block.

Modular arithmetic can be expressed in general terms by using letters in place of numbers. Conventionally the modulus is expressed as  $n$ , and within the context of encryption:

$p$  is used to represent the plaintext (the unencrypted text)

$c$  is used to represent the ciphertext (the encrypted text)

$K$  is used to represent the key.

So the general algorithm for the encryption process using modular addition becomes:

$$p + K \equiv c \pmod{n}$$

Remember, what this is actually saying is

$$p + K \pmod{n} \equiv c \pmod{n}$$

so you should be able to see that the left and right sides can be swapped to read

$$c \pmod{n} \equiv p + K \pmod{n}$$

Dropping the unnecessary 'mod  $n$ ' term from the left side gives us

$$c \equiv p + K \pmod{n}$$

which is the more usual way of expressing the general algorithm for the encryption process using modular addition.

## 2.3 Decrypting the Caesar cipher

As already explained, using the cipher wheel the decryption process simply involves displacing the outer wheel clockwise a number of places corresponding to the agreed key and translating each ciphertext letter shown on the inner wheel to its equivalent plaintext letter on the outer wheel. Using Julius Caesar's version of the cipher this would require a clockwise displacement of three places. I hope you can see that this would be just the same as displacing the outer wheel 23 places in an anticlockwise direction. This is because a displacement of 26 places in either direction is the equivalent of no displacement at all, so an anticlockwise displacement of 23 (or  $26 - 3$ ) is the equivalent of a clockwise displacement of 3. Thus 3 and 23 form a complementary pair since a mathematical operation using 3 (encryption), followed by a mathematical operation using 23 (decryption) would result in the original plaintext unaltered. In this example, 3 is the encryption key and 23 the decryption key. In general terms, keys are signified by  $K$  for the encryption key  $\overline{K}$  (read as K bar) for the decryption key.

### Activity 5.2 (exploratory)

See if you can write out the general mathematical expression for the decryption process of the Caesar cipher.

#### Comment

Mathematically the decryption algorithm would be expressed as:

$$p \equiv c + \overline{K} \pmod{26}$$

### Activity 5.3 (self-assessment)

What are the decryption keys for the Caesar cipher with encryption keys of:

- (a) 10
- (b) 15
- (c) 7

#### Comment

The answers are at the end of this part of the block.

Although the mathematical expressions I have described for encryption and decryption using the Caesar cipher show the encryption key and the decryption key separately, in practice (as you have seen from Activity 5.2) one key is so easy to derive from the other that effectively they can be regarded as a single key. So if I know the encryption key I also know the decryption key, or I can decrypt the ciphertext by reversing the encryption algorithm. Encryption systems like this are known as **symmetric key systems** because effectively only a single key is involved in the encryption and decryption processes.

## 2.4 A simple transposition cipher

As I've already noted, a transposition cipher is, in effect, an anagram of the plaintext. But for an anagram to be classed as a cipher, it must have been created in some systematic way using a method that can be shared with the intended recipient so that it can be decrypted. There are many ways this systematic process can be done.

One way to create the transposition is to use a matrix of cells and to write the message a letter at a time in sequential cells across the matrix.

Encryption is performed by reordering the columns of the matrix in some systematic way and then reading off the result to produce the ciphertext.

This kind of cipher is known as a **columnar transposition cipher**. A possible approach to this task is for the sender and receiver to agree on a codeword and a way to reorder the letters in the keyword into an anagram. Let's say that the codeword is Tuesday and the agreed transposition is to reverse the order of the letters (YADSEUT) and then swap pairs of letters, starting at the right-hand end to produce the anagram YDAESTU. The number of letters in the keyword dictates the number of columns in the matrix, and the plaintext is entered into each of the columns (with the keyword at the top) a letter at a time working across the rows as shown in Figure 5.6(a). Any empty places in a row can be padded with redundant letters (the 'x' in my example). The columns are then reordered according to the keyword anagram as shown in Figure 5.6(b). The ciphertext is given by reading back the letters from the reordered matrix. Thus, in my example, the message *Mary had a little lamb its fleecy was white as snow* is encrypted as:

DHARYMAETLITALSITMBLAWCEEEFLEITWHASXOWSNAS

(a) First stage

T	U	E	S	D	A	Y
m	a	r	y	h	a	d
a	l	i	t	t	l	e
l	a	m	b	i	t	s
f	l	e	e	c	e	w
a	s	w	h	i	t	e
a	s	s	n	o	w	x

(b) Second stage

Y	D	A	E	S	T	U
D	H	A	R	Y	M	A
E	T	L	I	T	A	L
S	I	T	M	B	L	A
W	C	E	E	E	F	L
E	I	T	W	H	A	S
X	O	W	S	N	A	S

Figure 5.6

### Columnar transposition cipher

#### Activity 5.4 (exploratory)

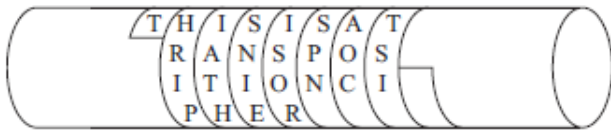
How do you think the intended recipient of the ciphertext produced by the matrix of Figure 5.6(b) would go about decrypting the message?

#### Comment

The recipient would reconstruct the matrix using the keyword anagram as the column headings, then reorder the columns so that the keyword returned to its original state. The unencrypted message could then be read off from the matrix rows.

There are many variations of transposition ciphers. One of the earliest recorded originated in Sparta in the 5th century BC. It used a wooden pole (or staff) known as a *scytale* (pronounced to rhyme with Italy). A strip

of parchment or leather was wound around the pole so that it formed a sleeve as shown in Figure 5.7. The message was written in rows along the length of the sleeve so that when it was unwound the letters of the message were transposed into a different order. To reconstruct the original message a pole of the correct diameter was needed.



**Figure 5.7** Transposition cipher using the Spartan scytale

## Answers to self-assessment activities in Extract 3

### Activity 5.1

(a)  $f = 5$

so when the key is 6, the calculation becomes

$$5 + 6 \equiv 11 \pmod{26}$$

The numerical value 11 represents the letter 'l', so the result of encrypting the plaintext letter 'f' with a key of 6 is the ciphertext letter l.

(b)  $s = 18$

so when the key is 12, the calculation becomes

$$18 + 12 \pmod{26}$$

But  $18 + 12 = 30$ , which is outside the range 0 to 25. Subtracting 26 from 30 leaves 4 so:

$$18 + 12 \equiv 4 \pmod{26}$$

The numerical value 4 represents the letter 'e', so the result of encrypting the plaintext letter 's' with a key of 12 is the ciphertext letter e.

(c)  $m = 12$

so when the key is 20, the calculation becomes

$$12 + 20 \pmod{26}$$

But  $12 + 20 = 32$ , which is outside the range 0 to 25. Subtracting 26 from 32 leaves 6 so:

$$12 + 20 \equiv 6 \pmod{26}$$

The numerical value 6 represents the letter 'g', so the result of encrypting the plaintext letter 'm' with a key of 20 is the ciphertext letter g.

### Activity 5.3

(a)  $\overline{K} = 16$  (because  $26 - 10 = 16$ )

(b)  $\overline{K} = 11$  (because  $26 - 15 = 11$ )

(c)  $\overline{K} = 19$  (because  $26 - 7 = 19$ )

## Extract 4

*Extract 4 is taken from Block 4 **Protecting and prying Part 1 Introduction to the block**. This part sets the scene for what is to follow in the rest of the block, so will give a good indication of the topics and issues covered in Block 4.*

### Section 1 Introduction

In June 2009, the UK government published a report called *Digital Britain* that emphasised the importance of appropriate understanding and appreciation of the ‘digital world’, and the need to plan and set out a programme of action for it. In their foreword to the report, the Rt Hon. Lord Mandelson and the Rt Hon. Ben Bradshaw MP said ‘We face changes that are transforming the world in which our businesses and people operate. The move from analogue to digital technology is one of those revolutionary changes. It will define the competitiveness of our economy and change dramatically the way we lead our lives.’ (Department for Business, Innovation and Skills, 2009, p. 1.) The report later makes the point that ‘personal data is the new currency of the digital world. Privacy and security of that data is an increasingly critical issue’ (p. 23).

This block focuses on aspects of this personal data, and in particular the need for, and availability of, mechanisms for protecting it, and the potential for individuals, government agencies and other organisations to use it to pry into our lives. In studying some of these issues you will need to confront not only the technology ‘fixes’, but also consider the more philosophical matters relating to human behaviour and priorities; these include for example, human rights and liberties, and the sort of society that we wish to live in.

### Section 2 Personal digital data

Few would disagree with the view that the transformation of our lives through digital technologies was already significantly underway long before the *Digital Britain* report was written. Indeed, the report itself acknowledges this when it says ‘On 15 June 2009, 20 hours of new content were posted on YouTube every minute, 494 exabytes of information were transferred seamlessly across the globe, over 2.6 billion mobile minutes were exchanged across Europe, and millions of enquiries were made using a Google algorithm’ (Department for Business, Innovation and Skills, 2009, p. 3). As digital technologies developed, and particularly over the preceding decade, they had been radically changing the way we communicate with each other, and the way we carry out many tasks in our personal and working lives, such as listening to and storing music, interacting with government agencies and purchasing goods.

Digital technologies are the greatest enablers of our time – and possibly even the greatest enablers of *all* time. For the most part, at the current time at least, individuals can choose whether or not to engage with them – no one is forced to have a computer in their home, to use a mobile phone or to receive digital broadcasts (though increasingly those who opt out are

liable to become disenfranchised and the refusal to receive digital broadcasts could result in no access to television). However, there is one key aspect of digital technologies that you will find impossible to avoid – that of the digital collection, storage and use of your personal information.

In the developed world, significant and insignificant events in our lives are digitally recorded, whether we wish it or not – our births, marriages, deaths, the schools we attend, the licences we are granted, the taxes we pay and the qualifications we achieve, to name but some. Even for those who choose not to use online or networked services, many of their interactions with the state – their claims for unemployment or disability benefits, for example – will still be recorded digitally, and their images are just as likely to be captured on security cameras if they are out and about in their local high street. All of these contribute to creating a digital identity that can say a lot more about us than our old ‘analogue’ identities did.

### Activity 1.1 (exploratory)

Give examples of two or three non-digital, physical documents you might use to prove your identity. What kind of information do they provide? How reliable is the proof they offer? How often over the last decade have you been asked to produce them? How do you protect them?

#### Comment

Here are the things I thought of:

Birth certificate. My birth certificate is handwritten on an official watermarked form (that clearly came from a book of blank forms because I can see evidence of perforations down the left-hand side where it was torn away). It has a printed identifying code consisting of two alphabetic and six numeric characters. It gives information on the date and place of my birth, my name, sex, the name, occupation and address of my father, the name and maiden name of my mother and the date my birth was registered. It also bears the name and signature (across a postage stamp) of the recording registrar. It would be difficult to falsify the information it

gives because the certificate’s identity code would enable the information to be cross-checked with the information recorded in the birth register. However, it’s a fairly easy matter for anyone with knowledge of some of the information recorded to obtain a replacement birth certificate, so possession of my birth certificate would not provide irrefutable evidence that the possessor is, in fact, me. I’ve only been asked to provide my birth certificate on two occasions over the last decade (when opening new accounts with building societies). I keep it in a locked filing cabinet at home.

Passport. My passport is a small booklet that includes an identifying code of nine numbers, my name, sex, date and place of birth, signature and photograph. Again, I think it would be difficult to falsify because the identity code would enable the information to be cross-checked with the recorded passport information. However, if my photograph could be replaced by a photograph of someone of similar age and same sex, it would be possible for someone in possession of my passport to masquerade as me (if they learned to forge my signature). I’m asked to produce my passport every time I travel abroad. Again, my passport is kept in a locked filing cabinet at home.

Driving licence. I still have one of the old-style UK licences, printed on watermarked paper. It includes a unique driver number consisting of some characters from my last name and other alphanumeric characters that I believe gives coded information on my date of birth. It also gives my full name and address, validity dates, details of licence type, several other alphanumeric codes, and a copy of my signature. There is a space to record endorsements. The information it gives could be verified against driving licence records. It would be possible for me (or anyone who has my details, including passport information) to apply for a new driving licence in my name, but this would be sent to my registered address, so in practice it might be quite difficult for someone to use it to masquerade as me. I can't remember an occasion over the last few years when I was asked to produce it, but in the days before bank cards, I used it frequently to verify myself when purchasing goods by cheque. I generally carry my driving licence with me.

Other documents you might have thought of are marriage certificate, utility bills, bank statements, student or work identity cards, certificates of achievement, contract of employment and work permit.

Activity 1.1 shows that, in the analogue world, there are numerous manifestations of our identity. Were it possible to gather together all the examples recognised, they would probably provide a fairly revealing profile, but individually they are quite limited. Gathering the information together would be a fairly simple task for the named individual, but an extremely difficult one for someone wishing to pry into their life or to masquerade as them. (When an organisation requests written evidence of identity it will often ask for several appropriate documents to be supplied, which makes deceit much more difficult.)

In the digital world there also exist myriad pieces of personal data that all make small contributions to our digital identities, but here there are two crucial differences. First, the opportunities for creating the data are abundant, and second, tracking them down and joining them together are much simpler, often requiring little expertise and no authority. Furthermore, digital technologies offer a much greater potential for prying as they capture the small details of our lives – the journeys we take, the goods we buy, the people we communicate with – and thus can provide a very revealing picture – not only of who we are but also of what we like, what we do and (sometimes) what we think. Some of this data we create willingly ourselves (for example through online social networking sites), some is created through our own complicity (for example through store loyalty cards and mobile phone use) and some is created for us, without us having any say or playing any part in the process.

This block takes a look at some of the circumstances in which personal digital data is recorded and used, and some of the mechanisms for protecting this data.

## Section 2 A thematic framework

As you study this block, in some of its parts you will be encountering five recurring themes, which together provide a framework that can be used for analysing the technologies you will meet:

- convenience
- identity
- reliability
- acceptability
- consequences.

In Sections 3.1 to 3.5, I use these themes to provide a further introduction to the ‘protecting and prying’ aspects relating to personal digital data.

### 3.1 Convenience

Although I’ve sounded a note of caution in earlier sections about digital systems that incorporate the use of personal information, there is certainly much to commend them in terms of convenience.

#### Activity 1.2 (exploratory)

Think about your own experience of systems that provide online access to information or services (for example, online banking). Identify two or three you use that rely on the use of some information that is personal to you. Make some notes about them in terms of convenience.

If you don’t use any online services that require you to enter personal information, spend a while thinking about the kind of services that you might find convenient to use and identify the personal information you think the organisations running them might require from you. Then compare your answers with mine.

#### Comment

I have identified three systems that I discuss below. Yours may be different, or you may have identified different reasons for finding them convenient.

Just a few days ago I arranged to pay my annual motor vehicle tax using the UK’s Driver and Vehicle Licensing Agency’s (DVLA) online service. Prior to the availability of this service, I would have had to take paper copies of my car’s current roadworthiness certificate – that is, its Ministry of Transport (MOT) certificate – and my current motor insurance certificate to a post office able to deal with motor vehicle taxation. I would have had to travel, and arrange my visit during post office opening times. Using the online service, I could complete the task from home in the evening. The receipt, in the form of a tax disc to display on my car windscreen, was sent to me by post two days later.

Online banking means I can pay bills and manage my account online. It enables me to transfer funds between accounts and view my account balance at any time I choose. It also provides me with access to other services, such as setting up and cancelling direct debits and opening new

accounts. Previously, if I'd wanted to do these tasks I'd have had to visit my bank's branch office during its opening hours.

I use the UK's online service provided by Her Majesty's Revenue and Customs (HMRC) to complete my income tax return annually. For me, there are two benefits that make this a convenient service. First, the tax I owe (or am owed) is automatically calculated as I complete the online form, so I get an instant indication of where I stand. Second, at the time of writing, the deadline for receipt of online returns is three months later than the deadline for paper returns, so I get extra time to complete the work. In this example, the convenience of flexibility of time and place isn't relevant because I could complete a paper tax return anywhere and at a time I choose (within the shorter deadline for return).

## 3.2 Identity

In the context of personal digital information, the issues of identity are multifaceted. In Activity 1.1 you looked at the kind of things you could offer as proof of identity in the analogue world. However, when I'm interacting with online services of the kinds I discussed in Activity 1.2, I can't offer my birth certificate or driving licence as evidence that I am who I say I am. So one aspect of identity is the means by which online systems verify my identity.

Another aspect is whether there are safeguards in place to ensure that someone else won't be able to impersonate me – an act known as identity theft. This could provide them with the means to access services they are not entitled to, to obtain control of my bank accounts, to pry into my personal information, or behave badly using my name and ruin my reputation.

Yet another aspect is the choice of personal data that is required and whether this is appropriate for the purpose. (Would you, for example, think it reasonable for your bank to ask you to provide information on your religion or sexual orientation?)

### Activity 1.3 (exploratory)

For each of the examples you chose for Activity 1.2, identify:

- (a) the personal information you are required to supply to verify your identity when accessing the system
- (b) additional personal information you think or know the system holds.

If you don't use any relevant online services yourself, use my examples and try to make some reasoned predictions at the answers.

### Comment

Here are my answers.

A short time before my motor vehicle tax was due for renewal, the DVLA sent me a form by post. This form showed my name and address, my vehicle registration number, make, engine capacity, and class. It also gave a reference number, which was the only information I was required to provide when I applied to renew online. Once there, the personal information details on the form were displayed, and I was asked to confirm them. In order to verify my vehicle complied with legal requirements, the DVLA must have had access to its MOT testing

information and my vehicle insurance details, which I had not been asked to supply. As the issuing body for UK driving licences, the DVLA will also have all the personal details that I was required to supply when applying for or renewing my licence, plus any licence endorsements that may have been added later.

When I access my online banking service I am required to provide a user identity code that was issued to me by the bank, a password I have chosen myself, and selected information from a second password, again that I have chosen myself. The additional personal information I believe the bank holds is my full name and title, address, date of birth and sex and, of course, a full record of my banking details including financial status and transactions.

To use the UK's HMRC income tax self-assessment online service I am required to provide a user identity code issued to me by HMRC and a password that I can choose myself. The additional information I believe HMRC holds is my full name and title, address, date of birth, sex, National Insurance number, tax code, employment details and history, full pay and tax details from previous years and any tax credits I claim.

### Activity 1.4 (exploratory)

When you analysed the personal information held by the systems discussed in Activity 1.3, were you surprised at its quantity and diversity? If all the information were joined together, what sort of picture of you would it give? How comfortable do you feel about this?

#### Comment

One thing that struck me was the way that organisations make my personal information available to other organisations. For example, the company that handles my motor insurance has made my details available to the DVLA and I have had no say in this (apart from having a voice in the electoral system appointing the government that introduced the associated legislation). This makes me concerned that I may not be aware of who has access to my personal information, and generally, I'd feel particularly concerned about any personal information that might put me in a bad light – for example, any road traffic violations or financial difficulties.

## 3.3 Reliability

An evaluation of reliability requires us to consider fundamental questions regarding security, accuracy and dependability. Will the system function as expected (and as claimed) and are there effective safeguards in place to monitor its performance? Also, is it open and transparent? When evaluating systems that handle personal data the main issue of reliability is whether it can be trusted by those whose data it handles and those who are using the system for particular purposes.

In the two or three years prior to me writing this introduction to the block, there have been numerous reports of leaks of personal information from various organisation's databases. At the time of writing – early July 2009 – the Open Rights Group lists as many as 39 what it calls 'UK Privacy Debacles' for the last six months alone (Open Rights Group, 2009). The reported data leaks have been so frequent that it would be easy to fill a

couple of pages with examples but I'll pick out just three of the very high profile cases to highlight the problem.

- January 2007. A security flaw on the TJX (the company that owns TK Maxx) computer systems was thought to have led to the theft of credit and debit card details of almost 46million of its customers (mostly in the US but some in the UK) over a period of about 18months (BBC, 2007a).
- November 2007. Two computer discs holding the personal details of around 25 million individuals were lost in transit between HMRC officials and the National Audit Office (BBC 2007b).
- January 2008. The details of 600 000 people (including bank account details of some of them) were stolen on a Ministry of Defence laptop taken from a car (BBC, 2008).

Time will tell whether lessons will be learned from these and similar, high profile, cases and whether, over the lifetime of this course, more robust protection methods are implemented so that the instances of potentially catastrophic data leaks such as those above will reduce in frequency and severity. (Perhaps this is something you might like to reflect on now.)

### Activity 1.5 (exploratory)

Take one of your examples from Activity 1.2 and list two or three questions you might like to ask about how reliably the system can protect your personal data.

#### Comment

I expect your questions relate to issues of privacy and accuracy, but you may have come up with others.

For my example I chose the DVLA's online service for paying motor vehicle tax and my questions are given below.

- How secure are my personal details, in particular the banking details I supplied for my online payment? How are they stored, and who has access to them?
- Are my details used for purposes that might put me at risk? (Recently concerns have been expressed about the DVLA's practice of selling data to private vehicle clamping companies (Times Online, 2009).)
- Are my personal details (those recorded by the DVLA itself and other organisations whose data it uses) accurate? Are there mechanisms for me to check their accuracy, and mechanisms for any inaccuracies to be corrected?

## 3.4 Acceptability

At the time of writing, the UK government is in the process of introducing a national identity card that it plans to make available to all UK citizens by 2012. This provides a good example to briefly explore some issues of acceptability.

The proposed identity card will show some basic biographical information (name, sex, place and date of birth and nationality), and some basic biometric information (a facial photograph and a copy of the holder's signature). The same information, plus fingerprint information, will also be digitally encoded and stored both in the card's chip and in a national identity register. In this way, the planned identity card will combine analogue identity data with digital identity data and will firmly tie together biographical data with biometric data.

Since the government's proposals were announced, there has been much public debate on the issue and various benefits and drawbacks of its introduction have been claimed. The National Identity Service says 'By locking one individual to one identity using their biometrics, the National Identity Service will make it much harder to create false identities. This will reduce the gains to be had from stolen identities. Once a person has their biometrics stored on the Register, they will be unable to claim an additional identity. This aims to make life easier and society safer.' (Identity and Passport Service, 2009). The government also claims the card will offer protection against terrorism, and will help to prevent fraud and illegal immigration.

On the other hand, pressure groups express concern about loss of privacy, cost (both to the individual and to the state), 'function creep' (that is, that the cards might at some time in the future be used for other purposes) and who will be able to have access to the data. At the time of writing, the UK's main political opposition party has pledged to scrap the proposed identity card system if it is successful in the next general election.

No doubt the eventual outcome of the proposed system will unfold during the lifetime of this course.

### Activity 1.6 (exploratory)

What are your own feelings regarding the acceptability of national digital database systems such as those operated (in the UK) by the DVLA, the Child Benefits Agency, the National Health Service, and the proposed identity card system?

#### Comment

Here are my own thoughts.

I'm aware that these systems may have the potential to protect me, by gathering information important for national security, for crime prevention and for health screening. So these digital data systems can help to make life simpler and safer for me and provide me with access to services – both state and private. But they come with a price. In order to enjoy the benefits they bestow I have to accept that my personal information is more readily accessible to individuals and organisations than it would have been a few decades ago. In other words, there is a trade-off between the benefits of protection and the drawbacks of prying.

I'm more inclined to accept the systems only when the benefits significantly outweigh the drawbacks.

An important point to bear in mind when considering acceptability is that it is not constant over time. It can be changed positively through use and practice, as experience of the system is built up, and through shifts in public perception as its use becomes familiar. However, it can also be changed negatively due to such things as security breaches and system failures and a consequent loss of public trust.

### 3.5 Consequences

Though the previous four themes can generally be considered in any order (and indeed this order is likely to vary in different parts of this block), consequences can really only be evaluated when all other issues have been examined. Even then, the introduction of new systems frequently leads to unforeseen results – both good and bad.

ICT systems are increasingly pervasive and ubiquitous and many of our day-to-day activities depend upon them. When they fail (or fail to behave as expected) the effects can fall anywhere on the continuum between inconvenience and catastrophe. So the adoption of big information systems needs careful thought and planning.

In my answer to Activity 1.6, I said I would be more inclined to accept digital data systems if the benefits significantly outweigh the drawbacks. What I should have added was 'now and in the future', for often the effects take a while to manifest themselves. Rights and liberties surrendered now are difficult to reclaim later, and big systems are difficult to reverse.

One of the obvious questions to consider is 'what might be the consequences when things go wrong?' What, for example, are the consequences of the breaches in data security that I identified in Section 3.3? It will probably take years for these to emerge and the full cost to be evaluated.

One less obvious question is 'what effect will the introduction of this system have on other systems?' For example, the shift to online services can be the death knell of traditional service provision, such as door-to-door postal deliveries, the provision of rural post offices and bank branch offices, and the option to pay for goods by cheque. Similarly, the shift towards online shopping will inevitably lead to less custom and therefore less choice in the high street. These moves can disenfranchise particular members of the community.

#### Activity 1.7 (exploratory)

This would be a good time to review your answer to Activity 1.2 and start to think about the possible consequences of widespread adoption of the systems you identified.

## Comment

I'm not going to attempt to make any comments on your possible answers to this activity. Its purpose was purely to prime your thinking for what is to follow rather than to come up with any robust answers.

## Section 4 Studying this block

This block uses two case studies – electronic voting and electronic banking – to place the use of personal information into a practical context. The first of these is introduced in Part 2, ‘Electronic voting’. This provides an early opportunity to help ‘sharpen your teeth’ and develop your critical thinking in relation to various ongoing proposals to replace traditional paper-based election processes with electronic, ICT-based, systems. The discussion of this case study is structured around the five themes you have just met in Section 3.

In Part 3, ‘Privacy and surveillance’, you will look at the debate relating to privacy and surveillance issues in the UK – generally believed to be the most intensively surveilled society in Europe and the Western world – before moving on to a more activity-based approach in Part 4, ‘Identity, authentication and authorisation’. Here you will explore some opportunities for controlling access to your personal information and you will be encouraged to consider aspects of your own online identity. (The material in this block is provided electronically, so you should plan to study this at a time when you will have access to a computer and internet connectivity.)

Protection is the major theme in both of the next two parts. Part 5, ‘Encryption’, will introduce you to methods used to protect sensitive or personal data by obscuring it – that is, by encoding it in such a way that it is only accessible to the intended recipient – and thus preventing unauthorised access. Part 6, ‘Biometrics’, looks at biometric security systems and their role in protection (in terms of both the state and the individual) and the issues surrounding their use.

The second of the two case studies is given in Part 7, ‘Banking on ICTs’, where many of the topics from previous parts are brought together and instantiated in practical applications. Here you will again meet the five themes of Section 3 used explicitly as a framework for considering electronic banking systems.

The final two parts of the block continue the skills development thread that runs through the course. Not only will these parts help to equip you with some of the skills needed to tackle the block assessment, they also provide development in some essential skills needed in the workplace. There are many occasions when ICT practitioners are required to communicate complex information in writing. (Indeed, you will be meeting some examples in Part 3 of this block where the substance of your studies is a series of readings taken from expert sources.) Part 8, ‘Writing longer reports’, builds on the report writing skills introduced in Block 2. It discusses the structure of long, formal reports, and provides guidance on how to plan and write them. Part 9, ‘Making good use of feedback’, discusses how to make use of feedback you receive on your work. Though the focus of this is on the feedback received on assignments, the same principles can be applied in wider contexts, and especially in the workplace.

## Extract 5

*Extract 5 is taken from Block 1 Storing and sharing Part 7 Writing technological documents. This part begins the development of written communication skills – particularly in a technical context – which is further developed at later points in the module. The section from which the extract is taken discusses particular characteristics of a written document that help the reader to engage with its content. Other topics in the same section (but not included with the extract) discuss style and technical level.*

### 3.3 Structure

The structure of a document depends on the medium. Documents on paper normally have a far more linear structure than documents written as a set of web pages. Documents intended for the Web are often – though not always – broken up into short sections, sometimes into single ‘screenfuls’, in order to make reading from the screen easier. In addition, they can incorporate links to many different pages or to all sorts of different resources. In this part of Block 1 I’ll concentrate on documents on paper (or destined for paper, even if created electronically).

The structure of a document also depends on the audience and the purpose. For example, if there are conventions about the structuring of a particular type of report then your audience will expect you to observe those conventions and will be surprised or even alienated if you do not. As another example, if you want your message to have impact, you may find that dividing it up into sections with well chosen headings helps. And so on.

Whether you decide to use sections or not, documents need structure. This is true even of short documents. The document should lead the reader through, with the ideas seeming to ‘flow’ from one to the next. This is not always easy to achieve, but you could use your purpose – and in particular the verbs in your purpose – to help you to decide on a structure. Here’s how.

Sometimes you may simply want to *state* something. One or two sentences are usually all that is needed to fulfil this purpose, and structure isn’t really an issue.

Sometimes you need to *list* the elements of something. Now you have to decide on the order of the elements in your list. Will the order be alphabetical, or by importance, or chronological, or ...? Once you have made that decision the elements of your list will probably be statements, so there are unlikely to be further ordering issues to deal with.

If your purpose is to *describe*, then your task is to examine various aspects of an object, phenomenon or event in turn. Once again, you need to decide on an order: the order in which you will tackle the various aspects. You could then write a paragraph for each aspect. But you will probably want to write more in these paragraphs than you did for items in a list, so you also have to think of a sensible order for the paragraph content. It’s helpful, though, to think first of what aspects you want to include and what order you want to present them in – that is, the order of your paragraphs – and only after you have made that decision go on to think

about how you present each aspect – that is, what you say in each paragraph.

If you are describing something big and complex then you may find that even a paragraph isn't enough to cover what you need to say about each aspect. In this case you probably need to use a separate short section for each aspect and then use the paragraphs in each section for sub-aspects of that particular aspect.

At this stage, I suggest you look at Figure 7.2, which is a visualisation of the various structures I am introducing. I've shown 'state' as one thin line, representing just a little text, and 'list' as several thin lines one under the other, representing several short items of text. The lines for 'describe' are thicker, implying that these are likely to be substantial paragraphs, or maybe even short sections, rather than just a line or two.



**Figure 7.2 A visualisation of structures for the purposes 'state', 'list' and 'describe'**

A frequent purpose is to *explain*. Explanations go beyond descriptions. They do not just say what something is like; they say why it is as it is, or how it got to be as it is. They usually include words such as 'because', 'therefore', 'so', 'as a result', or they may mention the word 'reason' or 'reasons'. This provides some sort of interlock between the various aspects of what you write, as is shown in Figure 7.3(a), where the arrows suggest how the elements may fit together into the explanation.



**Figure 7.3 A visualisation of two structures for the purpose 'explain'**

Notice how each aspect (except the first) locks to the previous one. For instance, a response to 'Explain why employees are leaving earlier and earlier in the evening' could be:

- The company provides inadequate car parking space.
- This means that employees try to arrive early in order to find a space.
- Therefore they complete their expected number of hours earlier.
- And so employees are leaving earlier in the evening.

Notice the characteristic words of explanations: 'this means that', 'therefore' and 'so'. Each of these locks the statement to the preceding one. Notice also that the explanation ends up with a restatement of what was to be explained. This is often the case.

I have deliberately separated the aspects of the explanation out in the foregoing, but in practice the explanation would probably be put into a single paragraph, something like this:

The company provides inadequate parking space, which means that employees try to arrive early to find a space. Therefore they complete their expected number of hours earlier, and so they leave earlier in the evening.

Some types of explanation are simpler than this. These are where a list of reasons for a particular phenomenon is given. Figure 7.3(b) shows this simpler type of explanation. The first horizontal line in this depiction would be along the lines of ‘There are three reasons why ...’ and then each item underneath would be one of the reasons. As you can see, this sort of explanation has features in common with a list.

### Activity 7.6 (self-assessment)

Match items A, B, C and D below to the verbs ‘state’, ‘list’, ‘describe’ and ‘explain’.

A Introduction to the block

Data storage

Finding information online

Wired networks

Wi-Fi and wireless local area networks

Service-oriented architectures

Writing technological documents

B The wireless network in Room 133 comprises a wireless access point (WAP), seven desktop computers and a variable number of notebook computers.

The WAP conforms to the IEEE 802.11g standard and is connected into the company’s LAN.

The desktop computers are all fitted with Wi-Fi cards, again conforming to the 802.11g standard. Employees need a user name and password to access the network from these computers.

As Room 133 is used for hot-desking, employees often bring their notebook computers into the room. If the employee is logged into their notebook computer then the computer will seek out and automatically log into the wireless network when they enter the room. Visitors with notebook computers will, however, need authorisation in order to use the network.

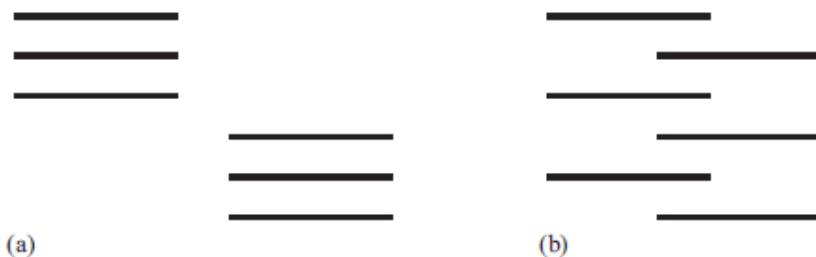
C There are two reasons why the wireless network in Room 133 sometimes slows perceptibly. First, when there are many users in the room, and some of them are accessing large files, the network becomes overloaded. Second, some notebook computers brought into the room still have 802.11b cards, and their use slows the room’s 802.11g network.

D The course title is *Communication and information technologies*.

### Comment

The answer is at the end of this part of the block.

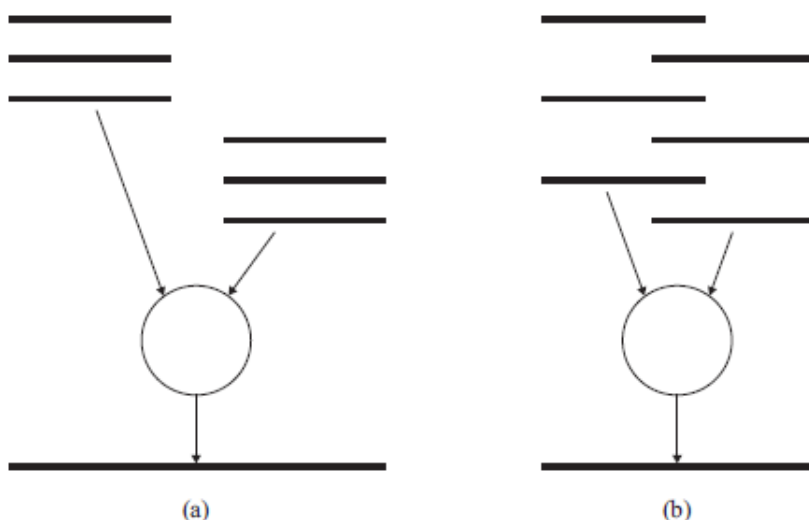
If you have been asked to make a recommendation then you will generally need to weigh up options. You will therefore find yourself comparing and/or contrasting aspects of the options. There are two principal ways of structuring a comparison or contrast. One, as in Figure 7.4(a), is to discuss all aspects of one option and then all aspects of the other. The other way, as in Figure 7.4(b), is to interleave the options, so that one aspect of both options is compared or contrasted, then another aspect, until all have been compared or contrasted. This structure works well when there is a direct pairing between all aspects, or when you have chosen a set of aspects to compare and/or contrast. When this is not the case the first structure may be preferable.



**Figure 7.4 A visualisation of two structures for the purpose ‘compare and/or contrast’**

Within both of the structures shown in Figure 7.4 you have a choice of the ordering of the aspects you are comparing and contrasting. It is common, but not universal, to group together ways in which the options are similar and ways in which they are different, rather than interleaving similarities and differences. But how you choose to order your comparisons and contrasts in any particular situation will depend on your purpose. For example, if your purpose is to persuade, then you may choose to work up to what you regard as your clinching point.

Once you have made your comparisons and/or contrasts, you need to weigh up the pros and cons in order to arrive at your recommendation. This is what the open circle in the depictions of ‘recommend’ in Figure 7.5 indicates.



**Figure 7.5 A visualisation of two structures for the purpose ‘recommend’**

You will probably be asked to *justify* your recommendation, which means you need to explain why you are making the recommendation. To do this you will need to make statements like ‘on such-and-such an aspect, this option is better than that option, because ...’ and ‘overall, therefore, it can be seen that this option is more suited to the company’s requirements than that option’.

The way in which you present your recommendation will be influenced by the purpose of your document. If you have been given a brief to make a recommendation, then you will probably feel that your overall purpose is to *inform* your audience and so adopt a dispassionate stance. But if you have chosen to make a recommendation because you feel some change should be made or some particular path followed, then you may well feel that you want your document to *persuade*. This may not affect your structure, but it will almost certainly affect how you put your points across.

You will probably seldom write a document where you have a single explanation or description. More often you will have several, and as I suggested above they may form parts of some sort of comparison and recommendation. In other words, your document may be quite complex. The box on ‘Separation of concerns’ has some suggestions to help here.

For all but the shortest documents, it can be a good idea to write some sort of introduction, even if only a sentence or two. This eases your audience into the topic. In a short document it may be as simple as ‘This document examines the problems customers have been experiencing with accessing the help-desk and suggests a possible solution.’ In a longer document it may consist of several paragraphs, but again it will give an overview of what is to come. In a report it may also summarise the brief given to those preparing the report.

Similarly, a conclusion, even if only a brief one, is helpful in all but the shortest documents, as it brings the document to a close in a way that’s satisfactory for those reading it. In fairly short documents it’s unlikely to be more than a summary of the principal points made. In longer documents it may also suggest further work that is needed.

Within a long document you may want to include some sort of ‘signposting’ – that is, brief statements that help your audience to see what’s coming or why you are discussing a particular topic. This could be as simple as saying ‘Each of these will be discussed in turn’ after you have listed some topics that are relevant to your document. Or it could take the form of ‘First’, ‘Second’, ‘Third’ at the start of appropriate paragraphs. You may like to look out for the ways in which other authors deal with this ‘signposting’ issue, as you may be able to learn from them.

#### Separation of concerns

When you start to plan the content of a document you will probably jot down many points you wish to make and topics you wish to include. This will be particularly so if your document is to be a long one. It can seem a long way from such jottings to a structure like one of the ones in Figures 7.2 to 7.5, especially as you may need to do a mixture of, say, stating, describing and explaining. An idea which can help you is that of ‘separation of concerns’. A ‘concern’ is simply a small topic that is made up of a set of points that ‘go together’. Your task in separating the concerns is first to identify your concerns – that is, your topics –

and second to group all the points you want to make under their most appropriate concern.

Of course, you may find some ‘awkward’ points that don’t fit neatly no matter how you try to group them. Often this is because they cut across two concerns. You may find you have to mention some points twice, in two different concerns. If this is the case, then you may be able to treat the point in less detail the second time you mention it, or you may choose to treat it in less detail the first time and mention that you will come back to it. Alternatively, with a bit of thought you may be able to use the point to help you to move on from one concern to another. Or you may simply realise that you haven’t chosen the most appropriate set of concerns – that is, the most appropriate groupings of ideas.

#### Activity 7.B1 (self-assessment)

- (a) What do you think the concerns are in the following extract?
- (b) Rewrite the extract to separate the concerns.

The use of VoIP would reduce the costs of international telephone calls, but all computers would have to be equipped with a headset and appropriate software, and not all members of staff would be comfortable with the headsets; at least it would mean one item less on everyone’s desk when we throw the phones away, though there is the problem that in a power cut we would all lose our phone line. At least the software is likely to be free.

#### Comment

One possible answer is at the end of this part of the block.

## Answers to self-assessment activities in Extract 5

### Activity 7.6

The matching is as follows:

- A list
- B describe
- C explain (note the word ‘reasons’ in the first sentence; this is a Figure 7.3(b) type of explanation)
- D state

### Activity 7.B1

- (a) My list of concerns is:

the resources needed (headsets and free software)

the benefits (reduced international call costs, fewer items on desks)

the drawbacks (discomfort with headsets, loss of phones during power cuts).

Your list may be somewhat different, but if it is distinctly different you may have misunderstood what a concern is, so look carefully at my answer and use it to help you to understand this concept.

(b) Here is one way of using the above list to rewrite the paragraph:

The use of VoIP would require all computers to be equipped with a headset. Software would also be needed, but is free. The principal benefit of using VoIP is cheaper international calls. Another benefit is that phones would no longer be needed, so there would be fewer items on the desks of staff. Two drawbacks of using VoIP are that staff may dislike using headsets and that there would be no phone service during power cuts.

Notice that a significant drawback at the end may cause the reader to take away a negative impression of VoIP. So, depending on purpose, it may be preferable to give the drawbacks before the benefits.

## Extract 6

*This extract gives an example of one type of TMA question you are likely to meet at the end of the first block of the module. This type of question enables students to build on the technical knowledge gained from their study of Block 1 (in this case wireless communication) by engaging with an article from a popular technology journal and carrying out a little additional research.*

*Support for the skills needed (written communication skills and information searching skills) are included in the Block 1 materials.*

### Question 2: the writing question

*This question carries 65% of the assignment marks.*

Imagine that you work for an ICT consultancy company. As a way to encourage customer loyalty, the company periodically provides a 'knowledge fact sheet' that it sends out to every customer who has used its services over the last two years. Each fact sheet is designed to explain a particular ICT technology to people who are not ICT professionals but who need to keep abreast of developments in ICTs.

The topic of the next fact sheet, to be sent out in late March, is to be wireless transmission of high-definition (HD) video signals, with particular focus on new wireless technologies designed to support this transmission.

Your task is to write the fact sheet. For your background information source you should find and use the article 'Wireless HD video heats up' by George Lawton. This article was published in the Technology News section of the IEEE journal *Computer*, volume 41, issue 12, December 2008, which is accessible through the Open University Library.

You should also search the Web to investigate whether the situation regarding the implementation of the new technologies has moved on since the article was written. But do not spend too long on this: if web-based technology news sources are not reporting anything significant in the last 12 months or so then you can assume there has been little or no change.

The fact sheet should include the following:

- a brief explanation of why there is a need to transmit HD video signals
- an explanation of why Wi-Fi (IEEE 802.11n) is considered inadequate for transmitting HD video signals
- a brief description of each of the two new technologies being proposed for transmission of HD video signals
- a statement of the advantages and disadvantages of each of these two technologies as compared with Wi-Fi (IEEE 802.11n).

It should also include a relevant and properly referenced quotation from the Lawton article.

## **Notes relating to Question 2**

The number of words must be between 450 and 500 excluding the reference list and text within any figures and tables.

In this question you need to 'role play' – that is, you need to write a fact sheet that not only meets the brief but also suits the specified audience and purpose.

You are strongly advised to follow the fourteen steps in Section 6 of Block 1, Part 7 to help you to prepare your answer to this question.