SCHOLAR Study Guide

Higher Computing Science
Unit 2: Computer systems

Authored by:

Ian King (Kelso High School)

Mark Tennant (Community School of Auchterarder)

Charlie Love (CompEdNet)

Andy McSwan (Knox Academy)

Reviewed by:

Jeremy Scott (George Heriot's School)

Previously authored by:

Jennifer Wilson (Denny High School)

Heriot-Watt University

Edinburgh EH14 4AS, United Kingdom.

First published 2018 by Heriot-Watt University.

This edition published in 2018 by Heriot-Watt University SCHOLAR.

Distributed by the SCHOLAR Forum.

SCHOLAR Study Guide Higher Computing Science: Unit 2

Higher Computing Science Course Code: C816 76

ISBN 978-1-911057-28-4

Print Production and Fulfilment in UK by Print Trail www.printtrail.com

Acknowledgements

Thanks are due to the members of Heriot-Watt University's SCHOLAR team who planned and created these materials, and to the many colleagues who reviewed the content.

We would like to acknowledge the assistance of the education authorities, colleges, teachers and students who contributed to the SCHOLAR programme and who evaluated these materials.

Grateful acknowledgement is made for permission to use the following material in the SCHOLAR programme:

The Scottish Qualifications Authority for permission to use Past Papers assessments.

The Scottish Government for financial support.

The content of this Study Guide is aligned to the Scottish Qualifications Authority (SQA) curriculum.

Contents

Topic 1

Data representation

Contents

Prerequisites

You should already know that:

- computers use binary code made up of ones and zeros to store integers;
- computers store text using ASCII code;
- computer graphics are stored as a series of bits corresponding to the number of pixels in the image.

Learning objective

By the end of this topic you will be able to:

- understand why computers store numbers as binary code;
- convert between positive binary and denary integers;
- understand how computers store integers using two's complement notation;
- convert between a denary integer and two's complement notation;
- describe the range of numbers that can be represented using a fixed number of bits;
- explain:
  - how computers store real numbers using floating point notation;
  - why text is stored as UniCode instead of ASCII;
  - the advantages and disadvantages of storing graphics as bitmaps or vector graphics.

1.1 Revision

Quiz: Revision Go online

Q1: Programs written in a High Level language need to be translated because?

a) Computers only understand machine code
b) Machine code is easier for the programmer to understand
c) There are many different programming languages
d) A computer can only understand a few programming languages

. . . . . .

Q2: There are many different High level programming languages because?

a) There are many different human languages
b) High level languages are often written to solve particular types of problem
c) There are many types of translation software
d) There are many different types of computer

. . . . . .

Q3: Explain how a bitmap graphic is stored.

. . . . . .

Q4: Which of the following is a vector graphics object?

a) Line colour
b) Polygon
c) Fill Colour
d) Coordinates

1.2 Using binary code to represent and store numbers

Learning objective

By the end of this section you will be able to:

- understand why computers store numbers as binary code.

Digital computers are made from millions (and often billions) of tiny switches called transistors. Switches can be either on or off. For this reason, all information handled by computers must be coded into/represented by patterns of 1s and 0s. Humans are much more familiar with the decimal system and think of numbers in terms of base 10, so in order to understand how the computer processes numeric information; we must be comfortable with both binary and denary numbers.

Decimal System

10^4	10^3	10^2	10^1	10^0	*	10^{-1}	10^{-2}
Ten Thousands	Thousands	Hundreds	Tens	Units	*	Tenths	Hundredths
0	1	3	5	6	*	0	5

We would read this as: $1 \times 1000 + 3 \times 100 + 5 \times 10 + 6 \times 1 + 5 \times 1/100 = 1356.05$

Like us, the computer must also be able to process positive and negative numbers that can also be very large or very small. This section looks at all such numbers and how they can be represented.

Quiz: Using binary code to represent and store numbers Go online

Q5: Why do you think we use a base 10 number system instead of 8 or 12 for instance?

We use the 10 symbols 0-9 to represent numbers in Denary, hence the reason we have columns that are expressed in powers of 10. Computers only have two symbols - 1 and 0 - so use columns that are expressed in powers of 2.

For example:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128s	64s	32s	16s	8s	4s	2s	Units
0	0	0	0	0	0	1	1

We would read this as: $1 \times 2 + 1 = 3$

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128s	64s	32s	16s	8s	4s	2s	Units
0	0	0	0	1	0	1	0

We would read this as: $1 \times 8 + 1 \times 2 = 10$

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128s	64s	32s	16s	8s	4s	2s	Units
0	0	1	0	0	0	1	1

We would read this as: $1 \times 32 + 1 \times 2 + 1 = 35$

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128s	64s	32s	16s	8s	4s	2s	Units
1	1	1	1	1	1	1	1

We would read this as: $128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255$ ($2^8 = 256$)

Since binary code can only consist of two values, 0 and 1, transmitting binary code is much easier and less prone to error than using a denary system where the numbers 0 to 9 would have to be represented by 10 different voltage levels. Although this may seem counter-intuitive to us who are used to the denary system, binary arithmetic rules are actually much simpler than denary ones, and therefore make processor design easier.

1.3 Storing integers

Learning objective

By the end of this section you will be able to:

- convert between positive binary and denary integers;
- convert between a denary integer and two's complement notation;
- describe the range of numbers that can be represented using a fixed number of bits;
- understand how computers store integers using two's complement notation;
- convert between a denary integer and two's complement notation.

You should already be aware of converting between positive binary and denary numbers from National 5. This section will recap this, and also introduce how computers store negative numbers so that we can convert those too.

1.3.1 Converting positive binary numbers to denary

Look at the method used to convert binary to denary in the interaction below. When you have finished this task, see if you can answer the questions which follow by using the method you have learned.

Example of binary to denary conversion

Look at the method used to convert binary to denary in the interaction below. When you have finished this task, see if you can answer the questions which follow by using the method you have learned.

Convert 10110101 to denary:

Step 1:

Draw out the column headings for this 8-bit binary number.

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Step 2:

Write in the denary values of each column.

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Step 3:

Insert the binary digits into each column.

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	0	1	0	1

Step 4:

= 128 + 32 + 16 + 4 + 1

=181

Q6: Convert 111 0110 to decimal

. . . . . .

Q7: Convert 011 0110 to decimal

. . . . . .

Q8: Convert 11 1101 1010 to decimal

. . . . . .

Q9: Convert 11011111 to denary.

. . . . . .

Q10: Convert 10100000 to denary.

. . . . . .

Q11: Convert 110011001100 to denary.

1.3.2 Converting positive denary numbers to binary

Example of denary to binary conversion

Look at the method used to convert binary to denary in the interaction below. When you have finished this task, see if you can answer the questions which follow by using the method you have learned.

1. Write down the column values at the top of the page.

2^4	2^3	2^2	2^1	2^0
16	8	4	2	1

2. Select the biggest column value that is not greater than your chosen number (in this case 16 is the largest value $<$ 29).

3. Put a 1 in the 16s column.

2^4	2^3	2^2	2^1	2^0
16	8	4	2	1
1				

4. Subtract 16 from 29, $29 - 16 = 13$.

5. Start again with the number 13.

6. Select the biggest column value that is not greater than 13 (in this case 8).

7. Put a 1 in the 8s column.

2^4	2^3	2^2	2^1	2^0
16	8	4	2	1
1	**1**			

8. Subtract 8 from 13, $13 - 8 = 5$.

9. Start again with the number 5.

10. Select the biggest number that is not greater than 5 (in this case 4).

11. Put a 1 in the 4s column.

2^4	2^3	2^2	2^1	2^0
16	8	4	2	1
1	**1**	**1**		

12. Subtract 4 from 5, $5 - 4 = 1$.

13. Start again with 1.

14. Select the biggest position value that is not greater than 1 (in this case 1).

15. Put a 1 in the 1s column.

2^4	2^3	2^2	2^1	2^0
16	8	4	2	1
1	**1**	**1**		**1**

16. Subtract 1 from 1, $1 - 1 = 0$.

17. Put a 0 in the empty columns.

2^4	2^3	2^2	2^1	2^0
16	8	4	2	1
1	**1**	**1**	**0**	**1**

$29 = 1\,1101$

Convert the following denary numbers to binary.

Q12: Convert 134 to binary

.....

Q13: Convert 148 to binary

.....

Q14: 29

.....

Q15: 18

.....

Q16: 79

.....

Q17: 273

1.3.2.1 Extension: Another method

The method shown below is another way of converting numbers into binary. Although it may seem more complicated it is actually very useful —you would likely use this method at university when studying Computer Science. Why? Because you can actually use it to convert a denary number into any base number system like Octal (powers of 8) or Hexadecimal (powers of 16).

Method 2:

Keep dividing by 2 and writing down the remainder until you are left with 0 then read the answer from the bottom up.

Convert 113 to binary
= 1110001

2	113	R
2	56	1
2	28	0
2	14	0
2	7	0
2	3	1
2	1	1
	0	1

Denary to binary conversion Go online

On the Web is a simulation of the repeated division method used to convert a denary number to binary. Using this interactivity you can enter your own numbers and test the conversions. You should now look at how this method works and then use it to convert some of the numbers from questions 12 to 21.

1.3.3 Range of positive integers

The range of positive integers that can be represented using n bits is **0..2^n-1**. You can see a pattern leading to this general formula in Table 1.1

Table 1.1

No. of bits	Binary patterns	Decimal values	Range
1	0, 1	0, 1	0..1 = 0..2^1 -1
2	00, 01, 10, 11	0, 1, 2, 3	0..3 = 0..2^2 -1
3	000, 001, 010, 011, 100, 101, 110, 111	0,1, 2, 3, 4, 5, 6, 7	0..7 = 0..2^3 -1

Q18: What is the range of positive integers that can be represented using 8 bits?

a) 0..16
b) 0..255
c) 0..256

. . . . . .

Q19: What is the range of positive integers that can be represented using 12 bits?

a) 0..24
b) 0..144
c) 0..4095

. . . . . .

Q20: The general formula for the range of positive integers for n bits is:

a) 0..2^n-1
b) 0..2^n
c) 0..2n-1

1.3.4 Representing negative numbers —Two's complement

Learning objective

By the end of this section you will be able to:

- understand how computers store integers using two's complement notation.

Remember: all information handled by computers is represented as patterns of 1s and 0s. We've now seen how any whole number can be represented by binary - but how about integers, which include a sign (negative and positive). How do we represent that in binary? Because all information handled by computers is represented as patterns of 1s and 0s.

One possibility might be to use an additional bit to represent whether the integer is negative or positive, a zero signifying a positive number and a 1 signifying a negative one. for example using 4 bits the numbers -1 to -7 could be stored like this:

+7	+6	+5	+4	+3	+2	+1	0	-1	-2	-3	-4	-5	-6	-7
0111	0110	0101	0100	0011	0010	0001	0000	1001	1010	1011	1100	1101	1110	1111

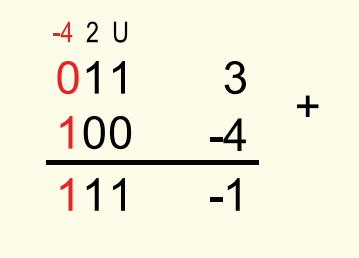
There are two problems with this method: we end up with two values, 1000 and 0000 which both mean zero, and using this system to add a positive number to a negative number gives the wrong answer as you can see from this example.

```
1011   -3
0100   +4   +
----------
1111   -7
```

The solution is to make the value of most significant bit (the leftmost column) negative instead of just representing a + or a - sign. In this example the most significant bit has a value of -4.

```
-4 2 U
 010   +2
 001   +1
 000    0
 111   -1
 110   -2
 101   -3
```

Addition now works when adding a positive and a negative number together and there is only one code for zero.



This system of representing integers is called **two's complement**. In two's complement notation, the most significant bit always has a negative value. This means that positive integers always start with a zero and negative integers start with a one. For this reason it is important to know how many bits are being used to represent a number in two's complement.

Quiz: Two's complement Go online

Q21: What two things can you tell about this two's complement number at a glance?
1000 1011

1.3.5 Converting negative decimal Integer into two's complement

Learning objective

By the end of this section you will be able to:

- convert between a decimal integer and two's complement notation.

There are 4 steps needed to convert a negative decimal integer to two's complement:

1. Establish the bit length required
2. Convert the positive version of the number to binary
3. Complement the binary number (ie. convert all 0s to 1s and vice versa)
4. Add 1

Examples

1. Convert -3 to 8 bit two's complement:

1.	+3 =	0000 0011
2.	Complement	1111 1100
3.	Add 1	+1
4.	**Result**	**1111 1101**

We can check this result: -128 + 64 + 32 + 16 + 8 + 4 + 1 = -3

. . . . . .

2. Convert -15 to 8 bit two's complement:

1.	+15 =	0000 1111
2.	Complement	1111 0000
3.	Add 1	+1
4.	**Result**	**1111 0001**

We can check this result: -128 + 64 + 32 + 16 + 1 = -15

. . . . . .

3. Convert -36 to 8 bit two's complement:

1.	+36 =	0010 0100
2.	Complement	1101 1011
3.	Add 1	+1
4.	**Result**	**1101 1100**

We can check this result: -128 + 64 + 16 + 8 + 4 = -36

Simulation of two's complement representation Go online

On the web is a simulation of the conversion of a 4-bit binary number to two's complement. You should now look at this simulation.

1.3.6 Range of Two's complement numbers

Range of numbers represented by two's complement:

Since one of the bits is now representing a negative value, the range of numbers you can store using two's complement representation is going to be placed on either side of zero rather than from zero upwards.

+7	+6	+5	+4	+3	+2	+1	0	-1	-2	-3	-4	-5	-6	-7	-8
0111	0110	0101	0100	0011	0010	0001	0000	1001	1010	1011	1100	1101	1110	1111	1000

Storing positive integers only using an 8 bit binary code would give you the range of 0 to 2^8 -1 ie. the range 0 to 255. In binary this would be 0000 0000 to 1111 1111.

However storing positive and negative integers using an 8 bit two's complement notation gives you a range -2^7 to 2^7 -1 ie. the range -128 to 127.

In two's complement notation this would be: 1000 0000 to 0111 1111.

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
-128s	64s	32s	16s	8s	4s	2s	Units
1	**0**	**0**	**0**	**0**	**0**	**0**	**0**

= -128

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
-128s	64s	32s	16s	8s	4s	2s	Units
0	**1**	**1**	**1**	**1**	**1**	**1**	**1**

64 + 32 + 16 + 8 + 4 + 2 + 1 = 127

Questions: Two's complete Go online

Q22: What is the range of two's complement numbers that can be stored with 6 bits?

a) 0 to 64
b) -32 to +31
c) -64 to +63
d) -32 to +32

. . . . . .

Q23: What is the range of two's complement numbers that can be stored with 10 bits?

a) 0 to 1024
b) -1024 to +1023
c) -512 to +512
d) -512 to +511

1.4 Storing real numbers

Learning objective

By the end of this section you will be able to:

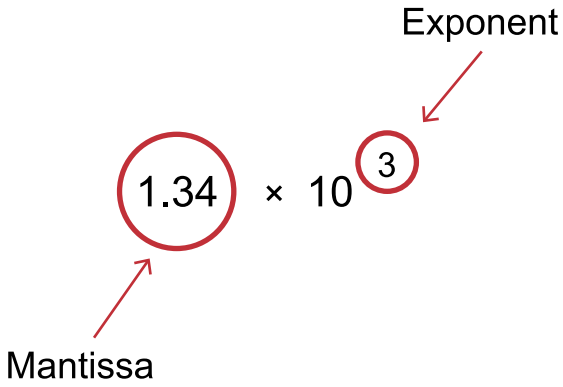
- understand how computers store real numbers using floating point notation.

A real number is a number with a decimal point. A real number can be positive or negative.

Decimal representation of real numbers uses a system known as scientific notation also known as standard form. Scientific notation allows us to represent very large or very small numbers using a short-hand where the number is represented by a value multiplied by a power of 10.

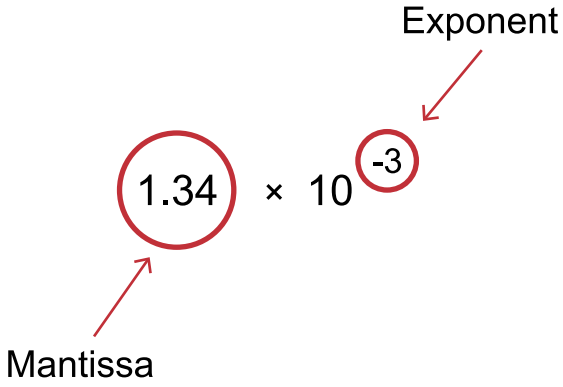
Scientific notation consists of three parts: the sign—positive or negative; the mantissa —a decimal number between 1 and 10; and the exponent —an integer representing a power of ten.

1340 can be represented as 1.34×10^3



The exponent can be positive or negative.

0.00134 can be represented as 1.34×10^{-3}



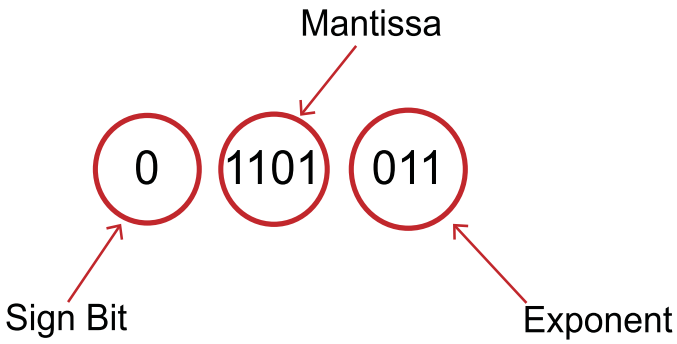
When very large or very small numbers are being represented then this system stores them with a limited degree of accuracy. This is an acceptable compromise because very large or very small measurements will not always be accurate to the same number of significant figures as would be needed to represent them as normal base 10 values.

Just as we have a denary point, the binary point works in the same way:

2^3	2^2	2^1	2^0	*	2^{-1}	2^{-2}	2^{-3}
8s	4s	2s	Units	*	1/2s	1/4s	1/8ths
0	0	0	1	*	0	1	1

Would be read as: 1 + 0.5 + 0.25+ 0.125 = 1.875

Computers use a similar system to scientific notation to store real numbers. This is known as floating point representation.



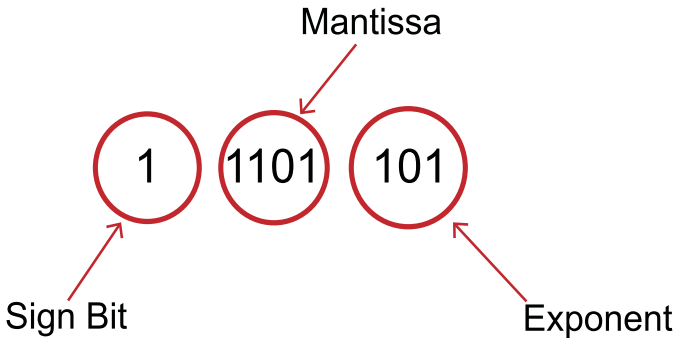
- The **sign bit** is a single bit, zero for positive and 1 for negative.
- The **Exponent** is a power of two stored in a system similar to **two's complement** notation because it can be positive *or* negative.
- The **Mantissa** is a positive binary fraction i.e. all the numbers to the right of the point (the point is not stored as the mantissa always starts with the first digit after it).

Just as we do with decimal scientific notation, when there is a negative exponent in floating point representation the binary point moves to the right. In this case it moves 3 places to the right.

In this example the number represented is:

$+ 0.1101 \times 2^{3}$

$= 0110.1$



In this example the number represented is:

$- 0.1101 \times 2^{-3}$

$= - 0.0001101$

A floating point number takes up more memory and requires more processing power to calculate than a two's complement number and may also be less accurate.

Range of numbers represented by floating point

The number of bits allocated to the exponent determines the **range** of numbers you can store. The exponent is an integer stored as a floating point number. If there were 8 bits allocated to the exponent this would mean that it could represent a range of numbers between 2^{127} and 2^{-128}

-128	64	32	16	8	4	2	U
0	1	1	1	1	1	1	1

= 127

-128	64	32	16	8	4	2	U
1	0	0	0	0	0	0	0

= -128

When a set number of bits is allocated to storing floating point numbers, there will always be a trade off between the range of numbers that can be stored (the exponent) and the accuracy with which they are stored (the mantissa). Floating Point Notation will always be a compromise between how accurately you can store a number and how large a range of numbers you wish to store.

Questions: Floating points Go online

Write down the binary number represented by the following floating point numbers. Assume 1 bit for the sign bit, 8 bits for the mantissa and 7 bits for the exponent (in two's complement format).

Q24: 0 11010001 0000100

. . . . . .

Q25: 0 11000000 1111100

. . . . . .

Q26: 1 10101111 0000110

Write down the floating point representation of the following binary numbers. Assume 1 bit for the sign bit, 7 bits for the mantissa and 4 bits for the exponent (in two's complement format)

Q27: 11.11001

. . . . . .

Q28: -0.0000011

. . . . . .

Q29: 110100.1

1.5 Storing text

Learning objective

By the end of this section you will be able to:

- explain why text is stored as UniCode instead of ASCII.

1.5.1 ASCII

With any system of storing data it is important to have a common standard. Common standards for storing data are important because it makes exchanging information between computer systems easier. It also makes the transfer of data between applications easier. Modern computer systems use two common standards for representing text: ASCII and Unicode.

ASCII (American Standard Code for Information Interchange) was originally developed in the 1960s for sending data over phone lines to electronic typewriters called teleprinters. As computer networks grew ASCII was also used to ensure all computers could read textual data sent between them.

Hex	Dec	Char		Hex	Dec	Char	Hex	Dec	Char	Hex	Dec	Char
0x00	0	NULL	null	0x20	32	Space	0x40	64	@	0x60	96	`
0x01	1	SOH	Start of heading	0x21	33	!	0x41	65	A	0x61	97	a
0x02	2	STX	Start of text	0x22	34	"	0x42	66	B	0x62	98	b
0x03	3	ETX	End of text	0x23	35	#	0x43	67	C	0x63	99	c
0x04	4	EOT	End of transmission	0x24	36	$	0x44	68	D	0x64	100	d
0x05	5	ENQ	Enquiry	0x25	37	%	0x45	69	E	0x65	101	e
0x06	6	ACK	Acknowledge	0x26	38	&	0x46	70	F	0x66	102	f
0x07	7	BELL	Bell	0x27	39	'	0x47	71	G	0x67	103	g
0x08	8	BS	Backspace	0x28	40	(	0x48	72	H	0x68	104	h
0x09	9	TAB	Horizontal tab	0x29	41	)	0x49	73	I	0x69	105	i
0x0A	10	LF	New line	0x2A	42	*	0x4A	74	J	0x6A	106	j
0x0B	11	VT	Vertical tab	0x2B	43	+	0x4B	75	K	0x6B	107	k
0x0C	12	FF	Form Feed	0x2C	44	,	0x4C	76	L	0x6C	108	l
0x0D	13	CR	Carriage return	0x2D	45	-	0x4D	77	M	0x6D	109	m
0x0E	14	SO	Shift out	0x2E	46	.	0x4E	78	N	0x6E	110	n
0x0F	15	SI	Shift in	0x2F	47	/	0x4F	79	O	0x6F	111	o
0x10	16	DLE	Data link escape	0x30	48	0	0x50	80	P	0x70	112	p
0x11	17	DC1	Device control 1	0x31	49	1	0x51	81	Q	0x71	113	q
0x12	18	DC2	Device control 2	0x32	50	2	0x52	82	R	0x72	114	r
0x13	19	DC3	Device control 3	0x33	51	3	0x53	83	S	0x73	115	s
0x14	20	DC4	Device control 4	0x34	52	4	0x54	84	T	0x74	116	t
0x15	21	NAK	Negative ack	0x35	53	5	0x55	85	U	0x75	117	u
0x16	22	SYN	Synchronous idle	0x36	54	6	0x56	86	V	0x76	118	v
0x17	23	ETB	End transmission block	0x37	55	7	0x57	87	W	0x77	119	w
0x18	24	CAN	Cancel	0x38	56	8	0x58	88	X	0x78	120	x
0x19	25	EM	End of medium	0x39	57	9	0x59	89	Y	0x79	121	y
0x1A	26	SUB	Substitute	0x3A	58	:	0x5A	90	Z	0x7A	122	z
0x1B	27	FSC	Escape	0x3B	59	;	0x5B	91	[	0x7B	123	{
0x1C	28	FS	File separator	0x3C	60	<	0x5C	92	\	0x7C	124	|
0x1D	29	GS	Group separator	0x3D	61	=	0x5D	93	]	0x7D	125	}
0x1E	30	RS	Record separator	0x3E	62	>	0x5E	94	^	0x7E	126	~
0x1F	31	US	Unit separator	0x3F	63	?	0x5F	95	_	0x7F	127	DEL

Example of first 128 ASCII characters

There is a big disadvantage with ASCII: as they only used one byte they were limited to 256 characters (the first versions actually only used 7 bits along with a 'check' bit for error detection, only allowing 128 characters!). This is not a problem for English languages, but what about languages with accents or different characters altogether such as Cryllic, Greek, Hebrew, Arabic, Chinese, etc. . . ?

To overcome this and allow more international characters to be represented a new standard called UniCode was agreed in the early 1990s.

1.5.2 UniCode

UniCode is the standard character format used by all modern devices. It originally used 16 bits to represent characters which allowed for a wide variety of foreign languages and symbols to be represented. More recently, 32 bits can be used which enables UniCode to represent every language (including historic ones like Egyptian Hieroglyphs) as well as symbols and a huge range of emojis used in online chat and social media.

By 2018 there were over 137,000 agreed characters making up the UniCode standard, with new additions recently agreed including the Mayan numerals (hey, you never know!) and flag emojis for Scotland, England and Wales.

UniCode Logo

Q30: What is the total number of characters that can be represented with 16 and 32 bits respectively?

Advantages of UniCode character representation

The adoption and use of UniCode has offered two main advantages:

- All current and historic languages can be represented and understood by all modern computing devices;
- The first 128 characters are identical to ASCII which maintains backwards compatibility with older files.

Disadvantages of UniCode character representation

Whilst UniCode is generally widely accepted, there are some drawbacks:

- UniCode takes up much more storage space than ASCII; 16-bit UniCode is twice the storage whereas full 32-bit UniCode is four times the storage requirements (hence it is rarely used in reality).
- The UniCode standard only defines what each number means and leaves it to software developers to decide precisely how each character looks on their system. You will most likely notice this if you compare emoji keyboards on Apple and Android devices, but it can cause issues with more common characters too.

1.6 Storing images

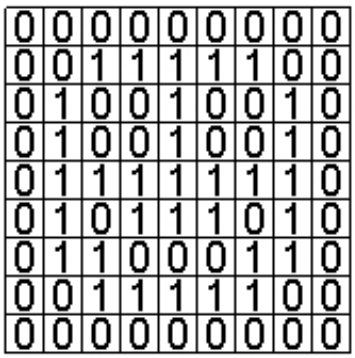
Learning objective

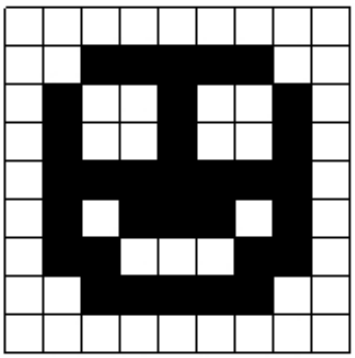
By the end of this section you will be able to:

- explain the advantages and disadvantages of storing graphics as bitmaps or vector graphics.

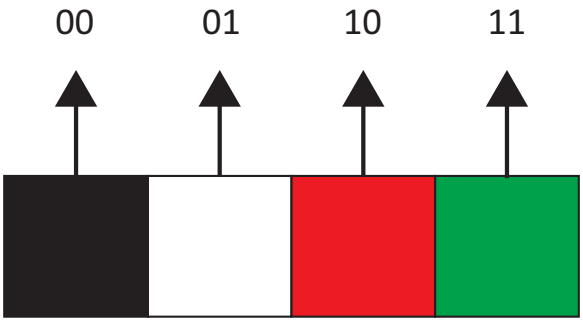
1.6.1 Bitmap images

A bitmap is a representation of a graphic using a grid of bits to store the information about the colour of each pixel in an image. Bitmapped images appear as pixels. Each pixel corresponds (or maps) to one or more bits in memory - hence the terms bit-mapped. A bitmap for a black and white image would be a simple grid with each bit representing whether the pixel was black (off) or white (on). For example this shows how this image would be stored using a 9×9 bitmap:





When using colours, multiple bits are stored for each pixel. The more bits user per pixel, the more colours can be stored.



Using two bits per pixel = 4 colours!

Allocating two bits per pixel would allow 4 possible colours to be stored. 3 bits allow 8 colours etc.

Experts agree that the human eye can distinguish up to 10 million colours (although an article in New Scientist in 2004 suggested that humans and other apes can distinguish around 2.3 million colours). If the true figure is indeed 10 million, then 24 bits per pixel would be required to represent this number (and significantly beyond, in fact). A bit depth of 24 bits (3 Bytes) per pixel would be required to store this amount of colour information. (2^{24} = 16,777,216)

File formats such as .JPG normally divide the 24 bits into three groups: 8 bits each representing red, green and blue values. These are the three primary 'additive' colours used by computer screens to produce their colour images. Some file formats (like .PNG) actually store 32 bits per pixel, with the extra 8 bits allowing them to store transparency values from 0-255 for each pixel.

Because bitmaps are made up of individual pixels it can be easy to use software to zoom in and edit individual pixels, for example removing red-eye from a photograph. However it is often difficult to re-arrange items in a bitmap image as the file format has no concept of the shapes or lines being shown —it is simply a grid of pixels.

1.6.2 Vector images

Vector graphics is an alternative method of storing graphics which stores them as a description of the shapes in the image to enable them to be re-drawn for recreating that image rather than storing them as individual pixels. There are two advantages of this system: vector graphics tend to take up much less disk space, and they do not lose resolution when enlarged, since their resolution depends on the device they are being displayed on rather than the device which created them. Because they are stored as a description, the disk space taken up by a vector graphics image will depend on the complexity of the image.

For example a rectangle could be stored as a set of attributes: start point coordinates, width, height, line colour, line thickness etc. A circle could be stored as a centre point coordinates, a radius, line colour, line thickness, fill pattern etc.

Because images stored as vector graphics use descriptions to recreate the image, they are not editable at pixel level in the same way as bitmapped images. Objects in a vector graphics application can be moved and resized independently of each other, whereas objects in an image created in a bitmapped graphics application will be stored as a number of pixels and cannot be manipulated as separate entities. Many bitmapped graphics applications use the concept of layers to get around this restriction. Each layer is a separate bitmapped image and each layer can be edited individually. Once the image is saved as a single bitmap however it can only be edited at pixel level.

Type	Advantages	Disadvantages
Vector	Can be scaled to large sizes, keeping original quality.	Difficult to create realistic images.
Suitable for graphic, unrealistic images and designs.	Individual objects can be edited, allowing an object to be altered without affecting the rest of the image.	Only individual objects can be edited (it is sometimes impossible to edit only part of the object).
	Are easily converted to bitmap formats.	Dependent on output hardware or software for appearance & quality.
	File sizes are relatively small.	
	Size of image can be increased keeping quality and file size the same.	
Bitmap	Images can be very realistic (e.g. digital photograph).	Scaling causes pixellation.
Suitable for natural, hand-drawn looking, realistic images.	Pixel level editing is allowed - allowing effects such as spray paint, blur, effects and so on.	Only the image as a whole can be edited.
	Same appearance in all systems, regardless of hardware or software.	Are very difficult to convert to vector formats, with unpredictable results
		File sizes can be large.
		Increasing the image size needs re-sampling and increases the file size.

Vector images Go online

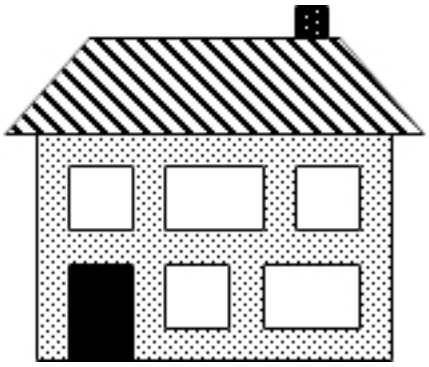
If you are not familiar with vector graphics from your previous studies, you should take time to explore the SVG grahpics format which is commonly used on the web. A tutorial can be found at https://www.w3schools.com/graphics/svg_intro.asp

1.6.3 Comparing bitmap and vector

At Higher level you are expected to be familiar with the advantages and disadvantages of each format. The next two activities will help you to compare the two formats.

Comparing bitmap and vector (20 min) Go online

1. Create a simple image like the one below in a **bitmap** package.



   a. Save the file **before you are finished** and make a note of the file size. Do this again when you are finished.
   b. Try to alter the fill colours, line thicknesses and position of the different shapes. Make a note of how easy or difficult this is.
   c. Zoom in and try to add details to the door such as a letterbox, number and knocker/doorbell. Again, note how easy or difficult this is.

2. Create the same image (or as close as you can) in a **vector** package.

   a. Save the file **before you are finished** and make a note of the file size. Do this again when you are finished.
   b. Carry out steps b & c from part 1 and again note down any issues.

3. Now compare your answers to the bitmap and vector tasks and explain to a partner or your teacher/lecturer why you think particular tasks were easier or hard in each package.

Bitmap and vector format Go online

Q31:

Decide whether listed points below are bitmap format (suitable for natural, realistic images) or vector format (suitable for graphic, unrealistic images, designs and drawings).

- Can be scaled to large sizes, keeping original quality.
- Size of image can be increased keeping quality and file size the same.
- Only individual objects can be edited (it is sometimes impossible to edit only part of the object).
- Scaling causes pixilation.
- Images can be very realistic (e.g. digital photograph).
- Individual objects can be edited, allowing an object to be altered without affecting the rest of the image.
- Pixel level editing is allowed —allowing effects such as spray paint, blur, effects and so on.
- Are very difficult to convert to vector formats, with unpredictable results.
- Only the image as a whole can be edited.
- Same appearance in all systems, regardless of hardware or software.
- Are easily converted to bitmap formats.
- File sizes can be large.
- Difficult to create realistic images.
- Increasing the image size needs re-sampling and increases the file size.
- Dependent on output hardware or software for appearance & quality.
- File sizes are relatively small.

1.7 Learning points

Summary

- Integers and real numbers:
  - computers store all data as binary numbers (base 2, using 0s and 1s); integers are stored using two's complement notation;
  - to convert binary into denary, write the binary number under its place values, then add;
  - to convert denary to binary, write the binary place values down, put a 1 in the largest place without going over your denary value, subtract this place then repeat for the remaining amount;
  - to convert a negative integer into two's complement, write it as a positive binary number using the full bit length, invert it then add 1
  - real numbers are stored using floating point representation;
  - floating point representation uses a mantissa, an exponent and a sign bit. The mantissa determines the accuracy of the number, the exponent determines the range of numbers which can be stored;
  - in a given number of Bytes, increasing the number of bits for the mantissa increases the precision of the number, but decreases the range;
  - In a given number of bytes, increasing the number of bits for the exponent increases the range, but decreases the precision.
  - A floating point number can be worked out by writing down the sign bit, the mantissa and the exponent required to move the digits to the correct position in relation to the binary point.
- Characters:
  - UniCode is a standard scheme for storing characters that commonly uses 16 bits (but can use 32);
  - UniCode uses more storage than ASCII, but allows a wider range of characters to be represented;
- Graphics:
  - Graphics can be stored as bitmaps where a 2D array of pixels is represented by a number of bits for each pixel.
  - Graphics can also be stored as vector instructions which store objects and their attributes to make up the image.
  - Bitmap images produce photo-realistic images which allow pixel-level editing but can produce large files.
  - Vector images produce small files and individual objects can be easily edited however they cannot represent photo-realistic images.

1.8 End of topic test

End of topic 1 test Go online

Q32: The denary number -73 (negative 73) can be represented in binary using two's complement by:

a) 1000 1101
b) 1011 0110
c) 1100 1001
d) 1011 0111

. . . . . .

Q33: What is the range of numbers that could be represented by a 12-bit Two's complement binary number?

a) 0 to +4096
b) -128 to +127
c) -2048 to +2047
d) -4096 to +4095

. . . . . .

Q34: When giving more bits to mantissa and fewer to exponent, which is true?

a) Accuracy increases, range increases
b) Accuracy decreases, range decreases
c) Accuracy increases, range decreases
d) Accuracy decreases, range increases

. . . . . .

Q35: A computer uses a floating point system consisting of 1 bit for the sign bit, 8 bits for the mantissa and 7 bits for the exponent. What would the fractional number -110.10100 be stored as?

a) 1 1010100 0000000
b) 1 11010100 0000011
c) 0 0000011 11010100
d) 0 11010100 1100000

. . . . . .

Q36: How many characters can Unicode represent if 16 bits are used per character?

a) 128
b) 256
c) 1024
d) 65536

. . . . . .

Q37: Approximately, how much storage is required to store a scanned A4 image (8.25 × 11.25 inches) at 300 dpi using a bit depth of 24 bits without data compression?

a) 200 MB
b) 85 MB
c) 23.9 MB
d) 0.7 MB

. . . . . .

Q38: Increasing the complexity of a vector graphic image:

a) increases the file size
b) decreases the file size
c) alters the object's attributes
d) displays the object more clearly

Topic 2

Computer structure

Contents

Prerequisites

From your studies at National 5 you should already know:

- the:
  - main components that make up a computer system;
  - three main parts of a computer processor;
- how:
  - memory is organised into locations;
  - data and address buses are used to link the processor and memory.

Learning objective

By the end of this topic you will be able to:

- describe the:
  - three main parts of a computer processor and their function;
  - roles of the Data Bus, Address Bus and Control Bus;
- explain how each is used during a memory read or memory write operation;
- describe how the computer retrieves and follows programs stored in memory using the fetch-execute cycle;
- explain how the following affect the performance of a computer system:
  - Number of processor cores;
  - Width of data bus;
  - Cache memory;
  - Clock speed.

2.1 Revision

Quiz: Revision Go online

Q1: The three main parts of a processor are:

a) Input, Process and Output
b) RAM, ROM, ALU
c) Silicon, Metal Pins, Socket
d) ALU, Control Unit, Registers

. . . . . .

Q2: Describe the purpose of the Data Bus in a computer.

. . . . . .

Q3: Memory locations are addressed using

a) Unique binary numbers
b) Postcodes
c) Random generated numbers
d) Unique Hexadecimal numbers

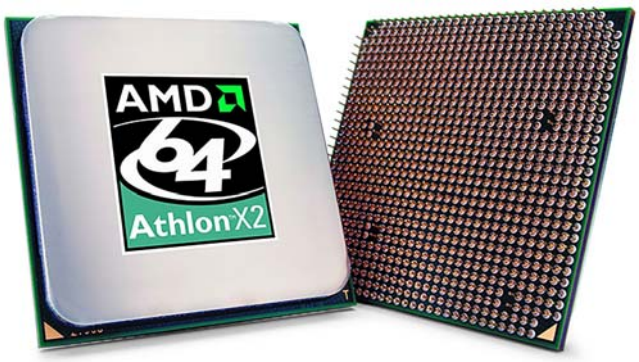
2.2 Parts of the processor

Learning objective

By the end of this section you will be able to:

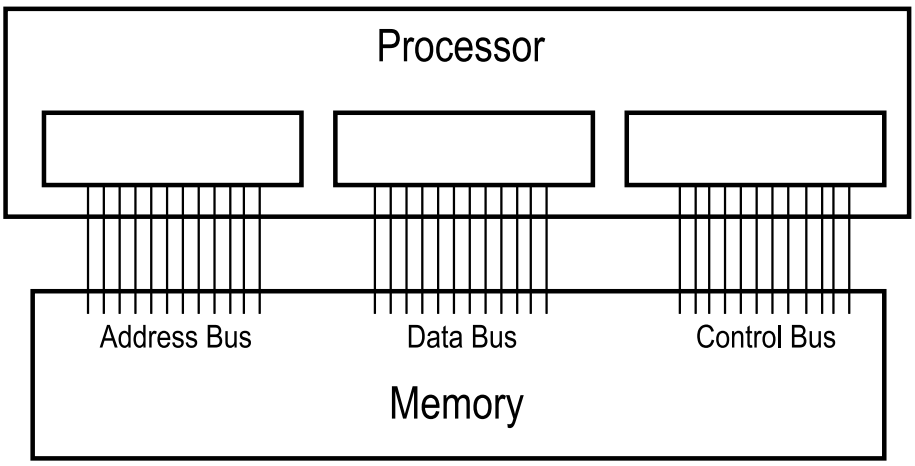
- describe the three main parts of a computer processor and their function.

If you have studied National 5 this section should mostly be revision. It is important however that you learn some common 'special purpose registers' that are not covered in the National 5 course.



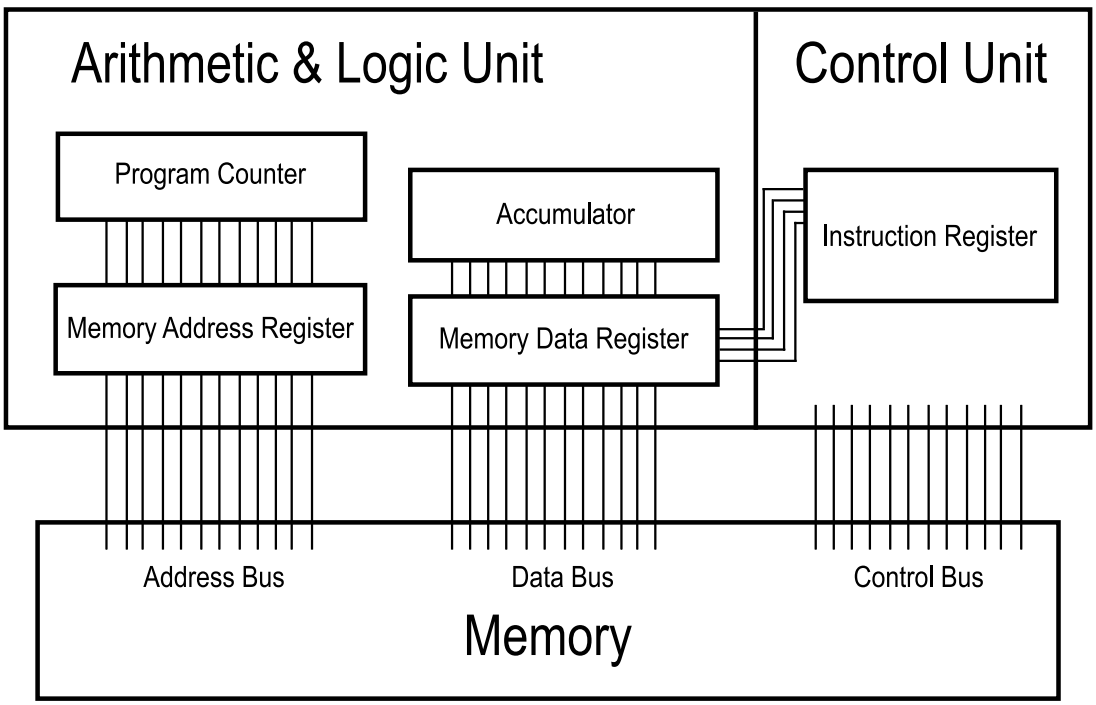
The CPU consists of several different parts: the Arithmetic and Logic Unit which performs calculations; the Control Unit which loads, decodes and executes instructions, and Registers which are small memory locations used by the processor.

Buses are the lines which connect the CPU to the main memory.



Registers are temporary storage areas in the processor which can be used to hold information such as:

- the address of the next instruction to be fetched (Program Counter);
- the address of the memory location where data is to be read from or written to (Memory Address Register);
- (intermediate) results of arithmetic and logic operations (Accumulator);
- data or instructions transferred between the CPU and memory (Memory Data Register);
- the current instruction being decoded and executed (Instruction Register).



2.3 Buses and their function

Learning objective

By the end of this section you will be able to:

- describe the role of the control, address and data buses in the fetch execute cycle.

The address bus is a unidirectional (1 way) bus, whilst the data bus is a bi-directional (2 way) bus.

When data is read from or written to memory:

- the processor sets up the address register with the address of the memory location to be accessed,
- the processor activates the read or write line on the control bus,
- and data is then transferred to or from the data register via the data bus.

Activity: Read and write operations Go online

Q4: Place each stage of the **read** operation in the right order:

- Read line is activated.
- Memory location is identified.
- Address of memory location to be read from is placed on Address register.
- Data is transferred to data register from memory location via data bus.

. . . . . .

Q5: Place each stage of the **write** operation in the right order:

- Write line is activated.
- Address of memory location to be written to is placed on Address register.
- Data is transferred from data register to memory location via data bus.
- Memory location is identified.

Each memory location has a unique binary address. Each line in the address bus can be on or off (1 or 0), so the total number of memory locations which can be addressed by the processor is

determined by the number of lines in the address bus.

The total number of memory locations will be 2 to the power of the number of lines in the address bus:

- 16 lines = 2^16 possible memory locations;
- 32 lines = 2^32 possible memory locations.

The Address and Data buses are sets of lines which work together to perform the same sort of function, however the control bus is really just a convenient name given to a collection of control lines including:

- Read line;
- Write line;
- Clock line;
- Interrupt line;
- Non-Maskable Interrupt line;
- Reset line.

Quiz: Buses and their function (10 min) Go online

Q6: The purpose of the address bus is to: (Choose one option)

a) initiate a read from memory operation.
b) carry a memory address from which data can be read or to which data can be written.
c) store results of calculations.

. . . . . .

Q7: The data bus is used:

a) to store the results of calculations.
b) to signal a read event.
c) transfer data between memory and processor.

. . . . . .

Q8: Why does the address bus not need to be bi-directional?

. . . . . .

Q9: How many memory locations could be addressed by a processor if it had a 24 line address bus?

. . . . . .

Q10: How much memory could be addressed by a processor if it had a 24 line address bus and a 16 line data bus? The data bus size means that each memory location would be 2 bytes long.

. . . . . .

Q11: What benefit would there be in adding additional registers to a processor?

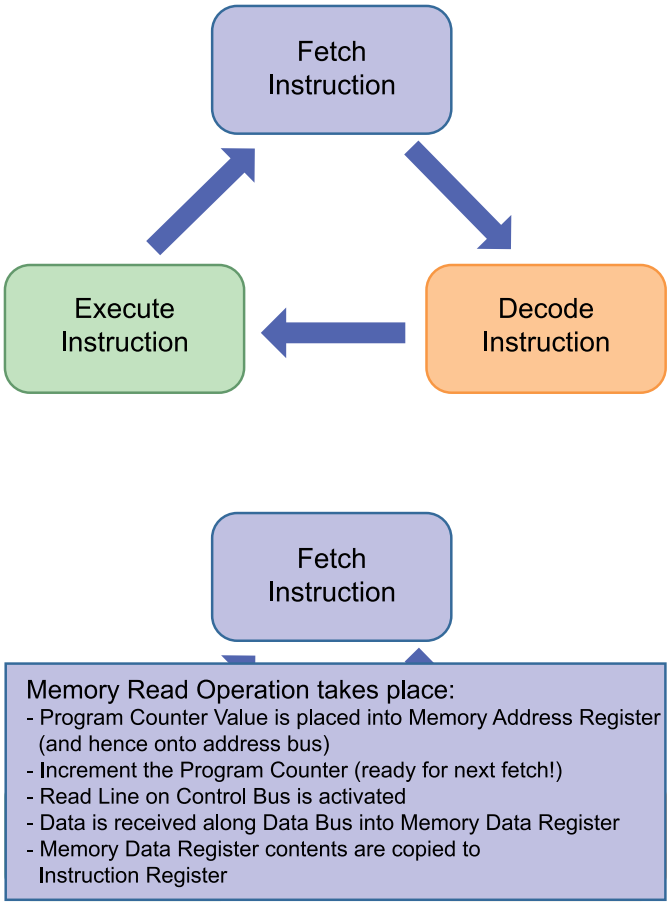
2.4 The fetch-execute cycle

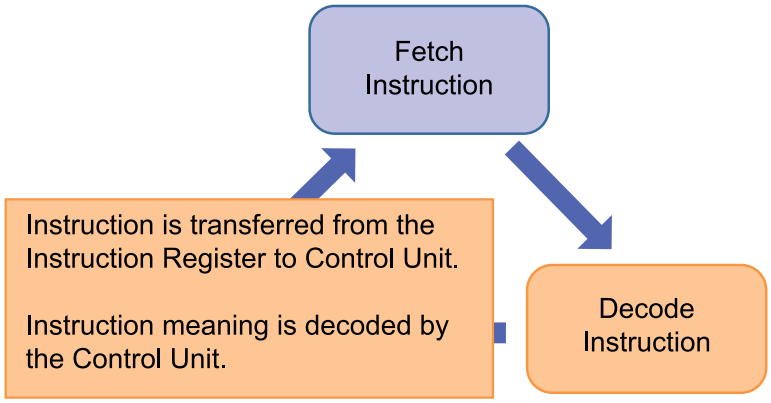
Learning objective

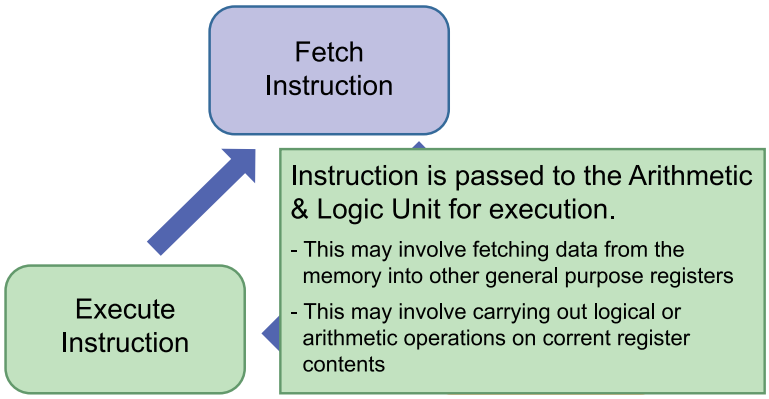
By the end of this section you will be able to:

- describe how the computer retrieves and follows programs stored in memory using the fetch-execute cycle.

The fetch-execute cycle is the set of steps which the processor takes when reading and executing an instruction. Such an instruction may be to read a piece of data from a location in memory and load it into a register; increment or add data to a register; or to write a piece of data to a memory location from a register.







The detailed steps are:

1. Transfer the contents of the Program Counter to Memory Address Register
2. Increment the Program Counter
3. Activate Read line (thereby transferring instruction to the data register)
4. Transfer contents of data register to the instruction register ready for decoding
5. Decode Instruction
6. Execute Instruction

The execute step might involve carrying out a simple instruction to increment a register; an instruction to load data from a memory location and add it to the accumulator; or an instruction to place a new memory location into the program counter.

Activity: Fetch-execute cycle Go online

Q12:

Place each stage of the fetch-execution cycle in the right order:

Note: of the following 9 stages, only 6 are correct.

	Transfer Program Counter to Memory Address Register
	Store instruction in accumulator
	Decode Instruction
	Increment the Program Counter
	Update control unit
	Execute Instruction
	Activate Read line
	Transfer data to memory address register
	Transfer instruction to Data Register and then to Control Unit

Quiz: Program counter (15 min) Go online

Q13: Why does the processor need a program counter as well as an address register?

2.4.1 Factors affecting system performance

Learning objective

By the end of this section you will be able to:

- explain how the following affect the performance of a computer system:
  - Number of processor cores;
  - Width of data bus;
  - Cache memory;
  - Clock speed.

In 1965, Gordon Moore (one of the founders of Intel) observed that the number of transistors that could be fitted on a silicon chip was approximately doubling every 18-24 months. Since then this observation has held true and has become known as Moore's Law. Moore's law stated that the number of transistors on integrated circuits is doubling every two years. This means that computing performance per unit cost doubles roughly every two years. So far Moore's law has held true, but the strategies for improving processor performance are limited.

Increasing the number of processor cores does not necessarily improve performance by the same amount as you might expect. Consider the following piece of code:

```
1. SET number1 TO 9
2.  SET number2 to 6
3.  SET number3 to 3
4.  SET total TO number1 + number2 + number3
5.  SET average to total/3
6.  SEND average TO DISPLAY
```

If you have a quad-core processor, lines 1-3 can all be executed at the same time (in parallel), as the order of execution is not important. The fourth core however could not process line 4, as this requires lines 1-3 to be completed first. In fact, lines 4-6 are very 'linear' in the fact that they all depend on the processing of the previous lines being completed. Running this program would take 4 clock cycles on a quad-core processor, not two as you may have presumed.

Research task: Factors affecting system performance (20 min) Go online

Using the web, find out how many processor cores are in a current laptop and a current tablet that are available for sale.

2.4.2 Width of data bus

Increasing the width (number of lines) of the data bus connecting the processor and memory allows for more data to be fetched in a single transfer. Data bus widths are often closely tied to the *word size* of a processor —that is how many bits of data the ALU and Registers are designed to cope with in one clock cycle.

A 32-bit data bus can transfer a 64-bit floating-point number to the processor, but this would take two transfer operations instead of one, halving the speed of these complicated calculations before we even factor in processor performance.

Most Desktop and Laptop computers have used 64-bit processors and data buses for some time, but it is a more recent development in mobile devices as the tables below show:

Intel Desk Processors

Year	Processor	Data Bus Width
1979	8088	8 bits
1982	80286	16 bits
1989	80486	32 bits
1993	Pentium	64 bits

Apple Mobile Processor

Year	Processor	Data Bus Width
2007	0098 (original iPhone)	32 bits
2010	A4 (iPhone, iPad)	32 bits
2013	A7	64 bits
2017	A11	64 bits

Note that, although 64-bit desktop processors have been around since the 1990's, it is only in the

2010s that software has been readily making use of this. Similarly, Apple devices made prior to 2013 are no longer able to install iOS updates due to the fact this is now a 64-bit Operating System.

2.4.3 Cache memory

Learning objective

By the end of this section you will be able to:

- describe how cache memory affects processor performance.

Although accessing Random Access Memory (RAM) is much faster than retrieving data from hard disk, processor performance can be improved by using cache memory. The cache is a faster kind of memory which stores copies of the data from frequently used main memory locations. The processor will use various techniques to improve performance using the cache including reading ahead in a program to load the cache with instructions which are likely to be needed soon. This technique is not foolproof, however, as user menu choices or branch instructions make it difficult to predict exactly which code will be needed next.

When writing to main memory the processor uses the cache to deposit data and then resumes its operations immediately. The data is transferred to main memory by the cache controller circuitry.

When reading from memory the processor first checks whether the information is already available in the cache memory. If so then it can transfer this at high speed to the processor. If not, then this step is a waste of time; however, more often than not, the information being sought is indeed in cache and the benefits in terms of access time can be quite dramatic.

Cache memory in modern systems often work with multiple areas —or 'levels' —of cache memory. Level 1 cache is built into the same chip as the processor and will give extremely fast access to data. Its capacity is limited however in order to fit the cache onto the same physical chip as the processor.

Level 2 cache is usually located between the processor and memory. Fast 'Static RAM' chips still provide much faster access to data than regular RAM, and are of larger capacity than level 1, but their speed will be slower compared to on-chip cache due to the delay in physically transferring the data to the processor.

Activity: Cache Go online

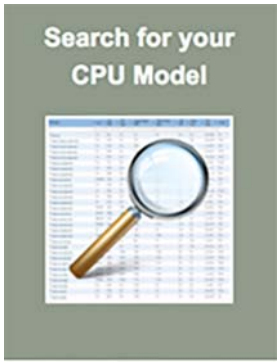
An interactivity showing an example of processor, cache and memory operations is available online

2.4.4 Clock speed

Increasing the clock speed of the processor means that more instructions can be executed every second. The disadvantage of this approach is that the power consumption and heat generated by the processor increases, so the cooling required becomes more and more complex and itself consumes more power. Modern supercomputers use super-cooled circuitry to reduce the resistance in their processors and increase their speed as a result. Even high-end gaming PCs for home use often resort to water-cooled processor systems nowadays.

While clock speed can be a useful indicator to computer performance, other factors like the number of cores, cache memory and complexity of instructions often have a wider bearing on performance in modern systems.

Go online: Clock speed Go online



1. Visit the website http://www.cpubenchmark.net which contains details of all major processors.
2. Scroll down until you find an option to search for a particular processor.
3. Now find 3 different computers for sale on the web. You should choose a budget laptop, a mid-range desktop and a high-end gaming/graphics editing machine.
4. Find out the models of the processors for each system (e.g. 'Intel Core i7-6850K').
5. Search for this on the cpubenchmark.net page and note down the clock speed and the 'Passmark CPU mark' (a type of benchmark test).

Think about the following questions when looking at your gathered results:

- What is the current speed of a typical computer processor?
- Do clock speeds and benchmark scores correlate with each other?
- Do you think 'Moore's Law' will continue to hold true in the future?

2.5 Learning points

Summary

- The Arithmetic & Logic Unit, Control Unit and Registers make up the main parts of a processor.
- The Processor is connected to memory using a bi-directional data bus and a unidirectional address bus.
- Read and Write lines on the control bus trigger memory-read and memory-write operations.
- The Fetch-Execute Cycle describes how a processor works through a program in memory: It fetches an instruction from memory (read operation), decodes the instruction in the Control Unit, then executes the instruction in the ALU. This process is repeated until there are no more instructions.
- The number of processor cores can improve the performance of a computer by processing instructions in parallel.
- Increasing the width of the data bus improves performance by allowing more data to be transferred between processor and memory each clock cycle.
- Cache memory can store blocks of memory contents in a faster area of RAM closer to (or on) the processor chip, which can increase performance.
- Increasing the clock speed of a computer will increase performance, but at the cost of increased power consumption and heat production.

2.6 End of topic test

End of topic 2 test Go online

Q14: Which statement fits into the blank area when describing the fetch-execute cycle?

- Fetch next Instruction by activating read line
- Transfer contents of memory data register to the instruction register
- _____
- Execute Instruction

a) Transfer Program Counter to Memory Address Register
b) Increment Program Counter
c) Decode Instruction
d) Prepare for execution

. . . . . .

Q15: The Instruction Register stores the:

a) Address of the next instruction
b) The instruction to be decoded by the processor
c) The program counter value
d) Result of a calculation

. . . . . .

Q16: Which of the following is NOT a way of increasing performance?

a) Increase the control bus width
b) Add more processor cores to the processor chip
c) Increase the data bus width
d) Increase the processor's clock speed

. . . . . .

Q17: Place these in descending order of access speed:

1. RAM
2. Hard Disk
3. Cache
4. Registers

. . . . . .

Q18: Increasing clock speed will improve performance but is not indefinitely possible because:

a) Intel need to hold speeds back so there is new technology to sell next year.
b) Heat generation and power consumption increase in line with clock speed.
c) Software will not cope with the increase speed.
d) No-one wants the increased processing power.

Topic 3

Environmental impact

Contents

Prerequisites

From your studies at National 5 you should already know that:

- energy use by computers can be harmful to the environment as much of our electricity generation comes from burning fossil fuels which produces the greenhouse gas CO^2;
- the energy used by a computer can be reduced by making use of:
  - Monitor settings;
  - Power-down options;
  - Standby settings.

Learning objective

By the end of this topic you will be able to:

- explain what is meant by an intelligent system;
- describe the environmental impact of intelligent systems in:
  - Heating systems;
  - Traffic control;
  - Car management systems.

3.1 Revision

Quiz: Revision Go online

Q1: Why can using computer systems be harmful to the environment?

a) People take less exercise as they are sitting at home playing games.
b) Computers can replace people in some jobs leading to unemployment, which forces people to take jobs in polluting industries instead.
c) Much of the electricity used by computers comes from non-renewable fossil fuels. Burning fossil fuels for electricity produces CO^2, a greenhouse gas.
d) The screens on a computer produce photons which can destroy the ozone layer.

. . . . . .

Q2: Which of the following actions would not reduce the carbon footprint of your computers?

a) Buying a more powerful processor.
b) Reducing the screen brightness.
c) Powering-down systems automatically every night.
d) Setting the computer to enter a standby state after 5 minutes of inactivity.

3.2 The Environmental impact of intelligent systems

Learning objective

By the end of this section you will be able to:

- explain what it meant by an intelligent system;
- describe the environmental impact of intelligent systems in:
  - Heating systems;
  - Traffic control;
  - Car management systems.

3.2.1 What is an 'intelligent system'?

An intelligent system is a machine that has ability to perform tasks that would require intelligence if they were performed by a human.

Examples of intelligence could be displaying one or more of the following attributes:

- Problem solving
- Creativity
- Learning from experience
- Reasoning and the ability to explain
- Vision
- Adapting to new situations
- Memory
- Natural language understanding.

Examples of intelligent systems could include robots that are built to act like humans and to perform human tasks, computer systems that can hold conversations as if they were human (expert systems), and computer systems that can play games and beat human opponents.

Expert systems are an area of intelligent systems that have been very popular. An expert system is a piece of software that attempts to take human knowledge about a subject and represent it using facts, rules and relationships. Answering a series of questions will allow the expert system to work through the rules and relationships to draw a conclusion. Whilst trying to encode facets of human experience and knowledge into a computerised solution can be difficult, the end results can be very accurate.

Q3: What is meant by the term 'intelligent system'?

Some areas of intelligent systems are now being used to help reduce energy use and emissions as concern over global warming grows. We will look at three areas in more detail:

- Controlling home heating systems
- Intelligent traffic control and management
- Car engine management

3.2.2 Heating systems

Intelligent systems are being used to change the way people heat their home. As well as saving energy, this can save consumers money too!

Traditionally, heating systems can be set with a thermostat and (usually) a timer. This can be inflexible, for example if someone living on their own goes out for the night, there is no need to keep the house at room temperature anymore.

Intelligent heating systems use and array of sensors and computer input to respond more dynamically to the situation in your home.

Smart Heating Thermostat from Nest.

The smart heating controller can make a number of intelligent decisions about your heating:

- Is your home occupied or not? Motion sensors or GPS data from your smartphone can feed into the system so that the heating is reduced when you are not at home. Some high-end systems can even use your smartphone location and speed to predict when you will arrive home and adjust the heating accordingly.
- Heating zones: sensors can detect which areas of your house are used at what times of the day and adjust the heating level of these areas accordingly.
- How will the weather affect your home? Data from weather forecasting can be used to predict when extra heating will be required, or if it may be best to shut it down altogether.
- Remote control: most smart heating systems can be connected to the internet, allowing you to manually adjust them via a smartphone app, regardless of where you are. Staying over at a friend's house for the night? No problem, just turn your heating down on your phone to save money.

You can read more about Smart Heating systems available in the UK here:

- https://www.honeywelluk.com/products/Underfloor-Heating/evohome-Main/
- https://nest.com/uk/thermostats/nest-learning-thermostat/overview/

Quiz: Heating systems Go online

Q4: How might a smart heating controller help you if your family go on holiday?

. . . . . .

Q5: How could a heating zone be used by a smart sensor in your home?

3.2.3 Traffic control

Intelligent systems are being increasingly used in traffic analysis and control.

Modern roads are covered in a network of sensors that can monitor traffic flow. These include speed sensors mounted in overhead cameras and 'induction loop' devices that can sense waiting traffic at junctions.

Computer systems can be used to make intelligent decisions based on the data from these sensors. Here are some examples of their current use in Scotland.

Variable speed limits

Several roads in Scotland now incorporate variable speed limit signs on overhead gantries. These are usually backed up by speed cameras to enforce the limit. The speed limit can be raised and lowered automatically by sensor input as well as historic data or can be manually controlled by a central control room in the event of an incident.

The aim of variable speed limits is to reduce queueing so that cars are not accelerating, decelerating then idling over and over again, producing greenhouse and other toxic gases.

Variable speed limit, Queensferry Crossing.
(Picture CC-BY-SA-2.0 M J Richardson/Geograph)

Traffic light management

Using data about waiting vehicles and number of vehicles on the roads, traffic lights can have their sequences altered automatically to prioritise busier routes. Traffic lights can also be networked together to share traffic data, so that progress of traffic can be maintained on a long city road by changing the signals at the correct times.

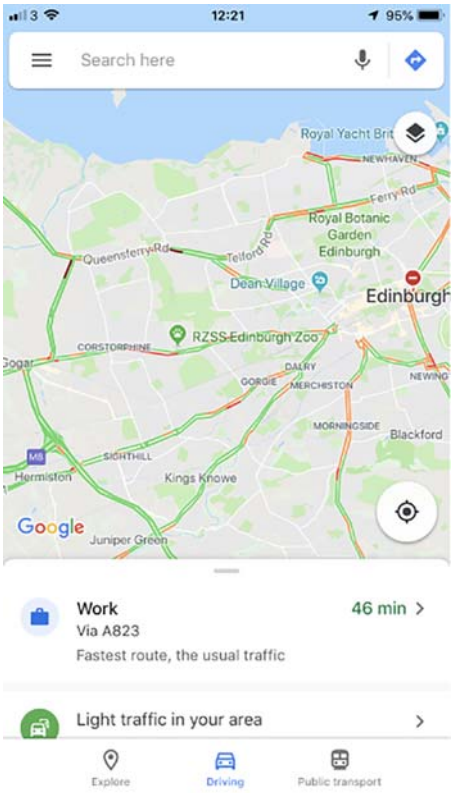
Photo of a 'smart' traffic light with pedestrian & traffic sensors

'Smart' pedestrian crossings now use a range of sensors to change their behaviour depending on traffic and pedestrian use. If an elderly or infirm person is taking a long time to cross they will stay on red until they are safely over, and conversely a quick crossing (or an abandoned one) will set the lights back to green for traffic again, minimising wasted time.

Traffic lights can also be set up to automatically prioritise bus lanes to encourage more public transport use, or can also change when they detect an approaching emergency vehicle displaying blue lights.

Traffic data in Sat-Nav apps

Road sensor data —along with GPS data from user's smartphones —can be used to help motorists plan journeys and avoid congested areas. As these are updated in real-time (provided you have a data signal) they can adapt the route taken as traffic conditions change.



Google Maps showing traffic data and recommended route to work

Increased use of more intelligent Sat-nav systems helps to reduce congestion and journey time, meaning less greenhouse gases and pollution released by queueing cars.

Quiz: Traffic control Go online

Q6: Which of the following may help reduce greenhouse gases?

a) Buying more cars, as long as they are modern ones.
b) Driving faster to reduce your time on the road overall.
c) Using up-to-date congestion information via an app to avoid queueing traffic.
d) Ignoring variable speed limits when the traffic is moving normally anyway.

3.2.4 Car management systems

Several intelligent systems are now being built into cars to reduce fuel consumption and emissions.

Start / stop technology

Modern cars now come with a feature built in that will automatically stop the engine from running when you are sat waiting in traffic. Electric pumps and motors will take over auxiliary functions like coolant circulation, air conditioning and fuel pumps while the engine is stopped. Sensors in the clutch (or brake pedal on an automatic) will detect when the driver goes to move off and start the engine in milliseconds. This is all controlled and monitored by an intelligent system that can differentiate between brief pauses in normal driving and having to stop for a period of time.

Some companies claim this can save as much as 10% of your fuel when driving in built-up areas with frequent stopping.

'Eco' mode

Many cars also come with an economy function that will reduce the engine power, giving better fuel economy. The system can usually be overridden (say, if carrying out an overtake) by fully depressing the accelerator, or if a sensor detects a steep incline.

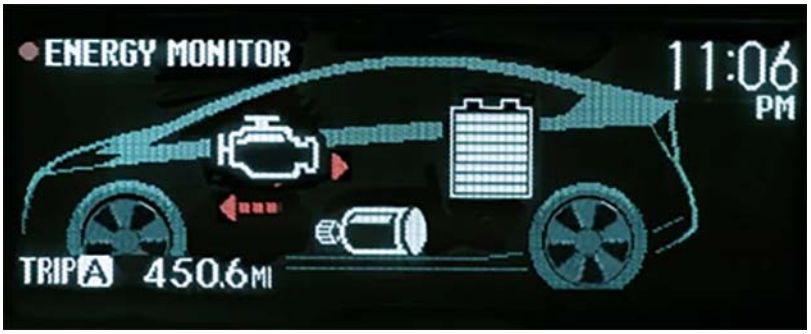
Intelligent Systems technology on a modern car: Start/stop mode, traction control, eco mode. The first and last options in this car will increase fuel efficiency when enabled.

Engine monitoring and control systems

Traditional petrol or diesel engines are now monitored by an array of sensors that make sure the combustion in the engine is as efficient as possible. They control valves and pumps in the engine to adjust the fuel/air mix going into the chambers and can react to changes in temperature, air and fuel quality to maintain an optimum mixture for the conditions.

Hybrid technology

Many cars now make use of electric power from a battery alongside traditional engines. This 'hybrid' technology can be used to lower vehicle emissions to benefit the environment. It requires a complex intelligent system to be constantly monitoring vehicle movement and driver actions through a series of sensors. Typically, the system will run the car on electric-only mode at low speeds, and use the normal engine for higher speeds. When decelerating or braking the system will use the 'wasted' energy from this process to recharge the battery.



Graphic from a Toyota Prius dashboard showing current energy use.

You can find out more about the hybrid technology used in some Toyota cars in this video: https://youtu.be/BZm3DVl3QNA

Self-driving cars

In the future increasing use of self-driving and highly-assisted driving cars may cut fuel consumption further. Self-driving cars are likely to be better at monitoring traffic flow and will make smoother acceleration and braking manoeuvres, saving fuel in the process. Integration with traffic data will also allow large groups of cars to adjust their speed as required to cut down on congestion and automatically re-route when needed.

You can read about leading-edge technology from Tesla here:
https://www.tesla.com/en_GB/autopilot

Assistive-driving technologies are already making an impact with features like adaptive cruise control (which automatically adjusts speed with traffic flow), speed sign recognition and gear-change indicators helping to reduce fuel consumption.

Quiz: Car management systems Go online

Q7: Apart from the environmental benefits of more intelligent systems in cars, what other benefits do you think they bring?

3.3 Learning points

Summary

- Intelligent Systems are computer systems that can make decisions based on a number of inputs. They typically mimic the sort of decisions that would normally require human intelligence to make.
- Smart heating can be used to make fine adjustments to your home heating setup based on occupancy, weather and GPS data to save energy and thus reduce CO2 emissions.
- Roads fitted with traffic sensors allow intelligent decisions to be made to control traffic lights and variable speed limits.
- Traffic data can be used by GPS systems and sat-navs to provide information about congestion and plan more efficient routes.
- A number of car management systems can be built into modern cars to increase fuel efficiency. These include engine monitoring systems, start/stop systems and hybrid power systems.
- Assistive-driving technologies are becoming more widely available that also help to make efficient use of fuel.

3.4 End of topic test

End of topic 3 test Go online

Q8: What is an Intelligent System:

a) A computer system that a human has to control all decisions in.
b) A computer system that can make human-like decisions automatically based on input from sensors.
c) A humanoid robot.
d) Any modern computer with a webcam connected to the internet.

. . . . . .

Q9: Why can smart heating systems benefit the environment?

a) They can help to reduce the energy used to heat a home by monitoring usage patterns, weather and owner's location.
b) They encourage home owners not to use heating.
c) Mobile apps to control heating allow you to turn up your radiators so the cat is nice and warm.
d) Only new houses can install smart heating systems, which are better insulated anyway.

. . . . . .

Q10: Which of the following intelligent systems would not help the environment when fitted to a car?

a) An engine start/stop function when stationary.
b) A hybrid power system.
c) Adaptive cruise control to match your speed to the vehicle in front.
d) A 'Sport' mode to increase acceleration performance.

Topic 4

Security risks and precautions

Contents

Prerequisites

From your studies at National 5 you should already know that:

- The General Data Protection Regulations (GDPR) require businesses to keep personal data about customers secure.
- Firewalls can be used to monitor and block activity between networked computers.
- Viruses, Worms and Trojan Horses can be used to attack computer data and introduce 'backdoors' into systems.
- Encryption is a process that can be used to scramble computer data into unreadable cyphertext that cannot be read without knowing the encryption key used.

Learning objective

By the end of this topic you will be able to:

- describe:
  - the impact of the Computer Misuse Act (1990) on individuals and businesses;
  - common faults caused by Denial of Service attacks;
  - how public-key encryption ensures secure transmission of data;
  - how digital certificates and digital signatures work;
- explain:
  - the security concerns around tracking cookies;
  - common symptoms, costs and effects of Denial of Service attacks;
  - the motives behind Denial of Service attacks.

4.1 Revision

Quiz: Revision Go online

Q1: What are companies who experience a data breach due to hacking required to do?

a) Keep it a secret in case other hackers try to do the same.
b) Inform the UK Information Commissioner within 72 hours.
c) Trace the hackers and perform a citizen's arrest.
d) Only tell customers if financial data is involved.

. . . . . .

Q2: How could a firewall help stop a hacking attack?

a) By only allowing data into your network on specific ports used by your software.
b) By making your computer untraceable.
c) By automatically carrying out a denial of service attack on suspected hackers.
d) By blocking all incoming data to your computer.

. . . . . .

Q3: What is meant by encryption?

4.2 Computer misuse and the law

Learning objective

By the end of this section you will be able to:

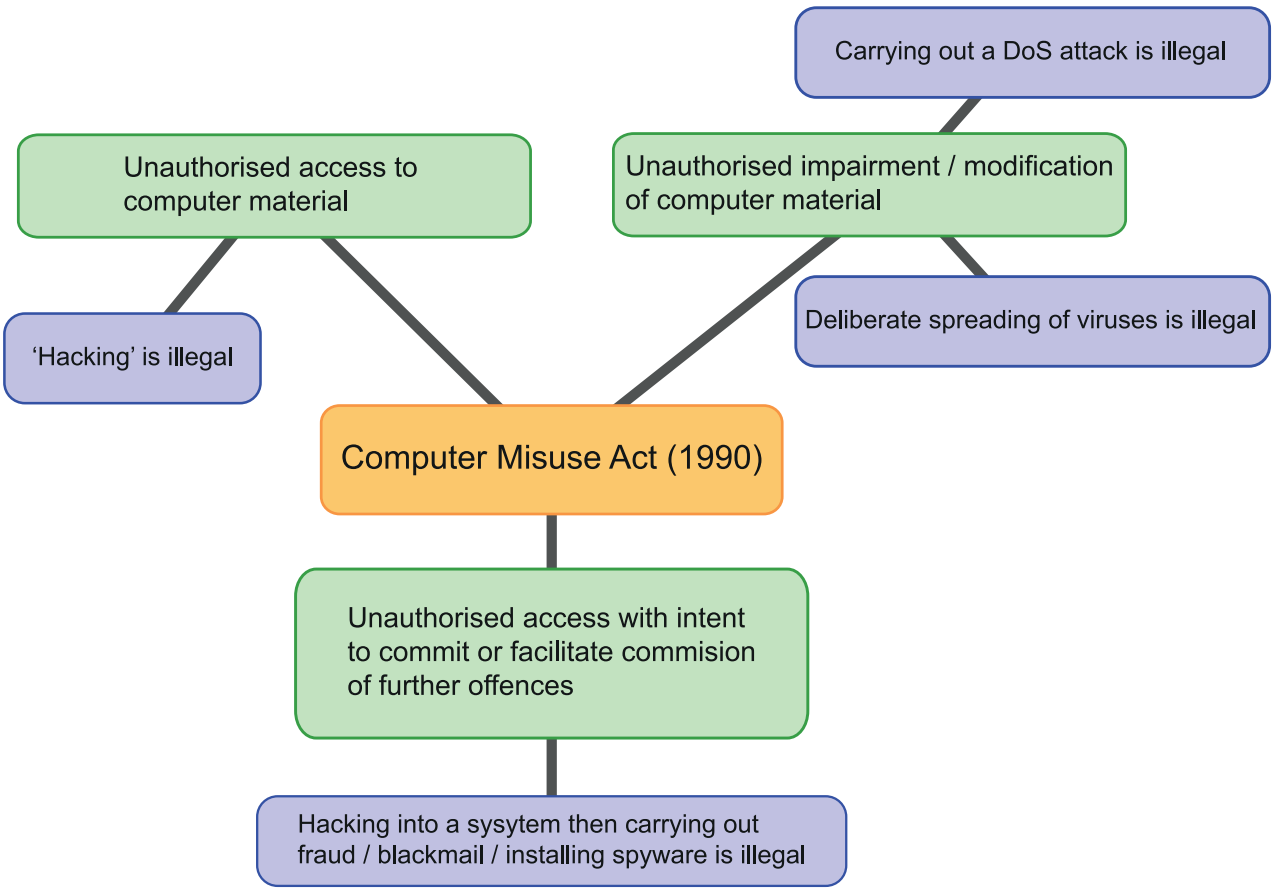
- describe the impact of the Computer Misuse Act (1990) on individuals and businesses.

From studying National 5 computing you will know that computers store a lot of information. Information can be a valuable resource and some users try to access this information without permission. This is generally referred to as 'hacking'. Gaining access to a computer system without permission, as well as altering or removing information without permission of the owner is illegal under the Computer Misuse Act. The Act refers to these acts as "unauthorised access" and "unauthorised modification". It also defines a more serious crime if you intend to commit further criminal offences through your access or modification.

The act created three specific offences:

- Unauthorised access to computer material.
- Unauthorised access with intent to commit or facilitate commission of further offences.
- Unauthorised acts with intent to impair operation of a computer.

The next sections will look at each offence in more detail.



Overview of the Computer Misuse Act (1990)

Q4: What is the name of the UK law which makes hacking illegal?

4.2.1 Unauthorised access to computer material

The first offence relates to any steps someone takes in order to gain access to a computer system.

An example of this type of offence would be guessing someone's password and using it to access a computer system to look at stored data. This is an offence even if no damage is done, and no files are deleted or changed. The act of accessing materials without authorisation is illegal. For example, copying a file from someone else's computer would not cause any damage to the file, but would be illegal.

Other examples might include:

- Using a Trojan Horse that allows remote access to search someone's hard drive over a network;
- Using a keylogger to steal a password for a co-worker or manager in order to view data you are not normally allowed to;
- Logging on with someone else's password to a computer system —even if it is easy to guess!

This offence carries a penalty of imprisonment up to six months and/or a fine.

4.2.2 Unauthorised access with intent to commit or facilitate commission of further offences

This builds on the previous offence. The key here is the addition of 'intent to commit '. It therefore includes guessing or stealing a password, and using that to access, say another person's online bank account and transferring their money to another account.

Other examples might include:

- Gaining access to a computer system and trying to change records that would benefit you or another person;
- Logging into the online banking system of another person and transferring money over to yourself;
- Gaining access to personal data or images and blackmailing the owner.

For this offence the penalty is up to five years' imprisonment and/or a fine.

4.2.3 Unauthorised acts with intent to impair operation of a computer

The last main part of the act deals with actions that can cause changes or damage to the computer's programs and data. Originally this was intended to deal with offences where people had deliberately destroyed data or had deliberately spread a computer virus with the intent of infecting other computers. More recently the idea of 'impairing' the operation of a computer was added to deal with more complex types of attack such as ransomware and Denial of Service Attacks (see section 4.4).

Examples of offences in this part of the act include:

- Deliberately spreading a computer virus. (though, simply writing a virus is not an offence on its own —prosecutors would have to prove you had the intent to cause harm);
- Gaining access to a computer system and deleting contents as part of a revenge attack;
- Deploying Ransomware software which encrypts users' data and asks for a sum of money to provide the key.

This offence carries a penalty of up to five years and/or a fine.

Activity: Computer Misuse Act Go online

Read the following example offences carefully and decide which part of the Computer Misuse Act they fall under.

Q5: Mary has had an argument with her manager and resigns. After leaving the company she logs in from home using her colleague's password (which she found out from a note in their shared desk) and deletes the customer contact database.

a) Unauthorised Access to Computer Material
b) Unauthorised Access with intent to commit or facilitate commission of further offences
c) Unauthorised acts with intent to impair operation of a computer

. . . . . .

Q6: Singh has recently failed a test in his school. When the teacher leaves the room briefly, he can't believe his luck as the teacher has left the school's marking system open on his computer, which is protected with a password written under the monitor. Singh quickly enters a 'pass' into his result entry and presses 'submit to exam board'.

a) Unauthorised Access to Computer Material
b) Unauthorised Access with intent to commit or facilitate commission of further offences
c) Unauthorised acts with intent to impair operation of a computer

. . . . . .

Q7: Singh's classmates are equally amazed and Lucy steps forward to look. She searches in the teacher's documents and finds a list of the last test scores for the whole year. She reads these out, much to the embarrassment of some of her classmates!

a) Unauthorised Access to Computer Material
b) Unauthorised Access with intent to commit or facilitate commission of further offences.
c) Unauthorised acts with intent to impair operation of a computer

. . . . . .

Q8: Daniel works for an environmental company who are campaigning against a new bypass. He suspects the builder is planning to ignore certain environmental requirements in the approved plans. During the night he manages to gain access to the builder's yard and installs a 'keylogger' device on the foreman's computer, which he then retrieves the following night and uses it to view and copy the foreman's files.

a) Unauthorised Access to Computer Material
b) Unauthorised Access with intent to commit or facilitate commission of further offences.
c) Unauthorised acts with intent to impair operation of a computer

. . . . . .

Q9: Rebecca has recently completed a cyber security course in college and boasts how she is so much safer than her peers now. Robert decides to teach her a lesson and sends her a message with a link to a 'cool new game' —this turns out to be a virus which stops some of Rebecca's programs working properly.

a) Unauthorised Access to Computer Material
b) Unauthorised Access with intent to commit or facilitate commission of further offences.
c) Unauthorised acts with intent to impair operation of a computer

. . . . . .

Q10: Chris finds a wallet dropped in the street. He checks through it and notices a small card with online banking details written on it. He tries these on his smartphone and they work! Not only that, the account has tens of thousands of pounds in it. Chris decides the owner probably won't notice £500 missing and so tries to transfer this to his own account. Unfortunately, the bank sends a 'one-time passcode' to the account's owner which the transfer won't go through without.

a) Unauthorised Access to Computer Material
b) Unauthorised Access with intent to commit or facilitate commission of further offences.
c) Unauthorised acts with intent to impair operation of a computer

4.3 Tracking cookies

Learning objective

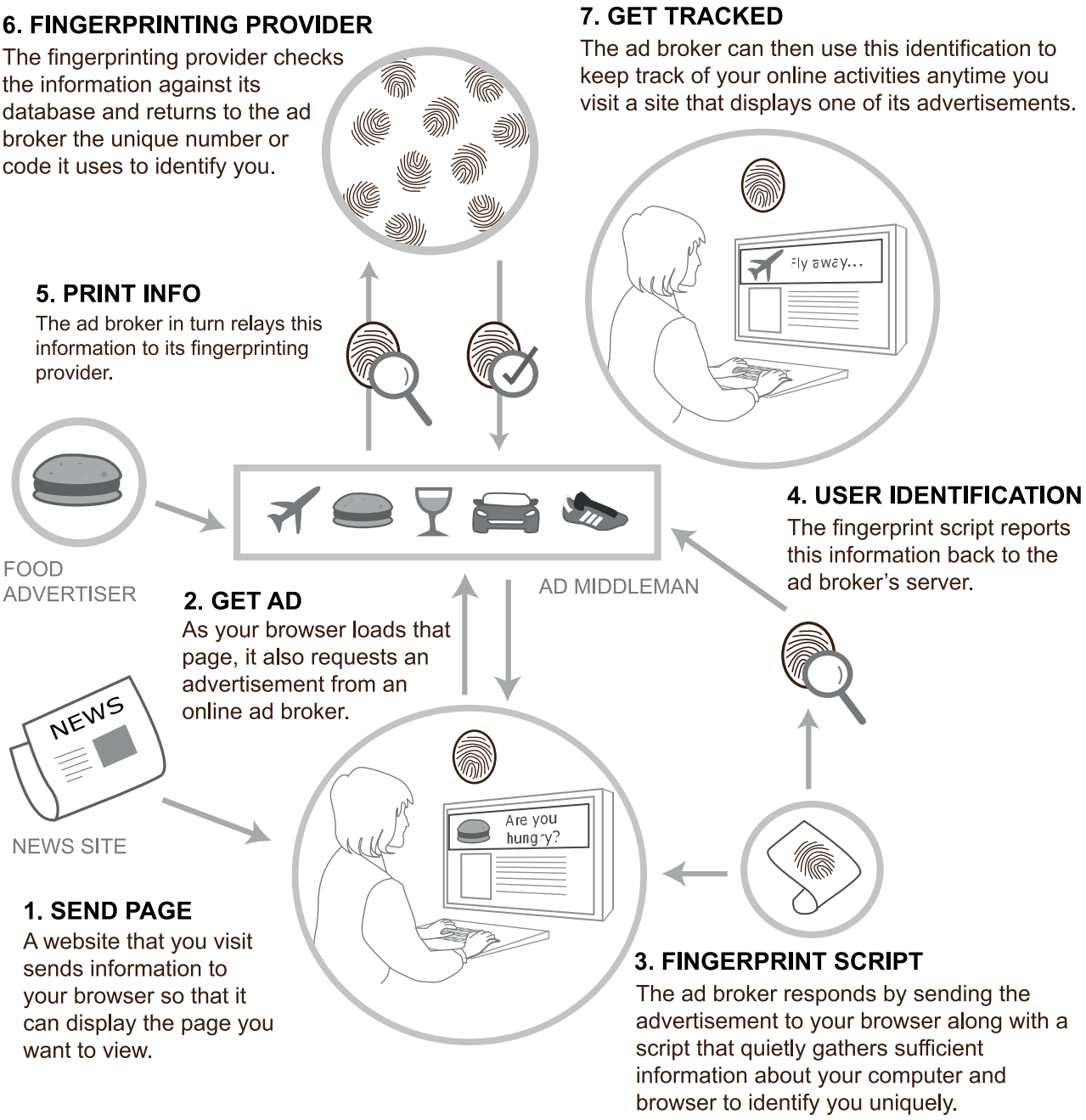
By the end of this section you will be able to:

- explain the security concerns around tracking cookies.

Cookie tracking, cookie profiling or web profiling is the use of persistent or permanent cookies to track a user's overall activity online. This tracking does not just happen when you are on a particular site, but it occurs the whole time you are browsing. This kind of profiling activity is often done by marketers who buy advertising rights on thousands of popular websites in order to collect and collate cookie information and create a single "profile" of a user.

Internet advertising, as it is called, targets potential customers based on the way they browse the Internet. This is the very reason why most websites flash banner ads on their pages. This matter may not be a big deal for some, but others take their privacy seriously and are uneasy about being "followed around" and profiled.

Figure 4.1: Cookie tracking

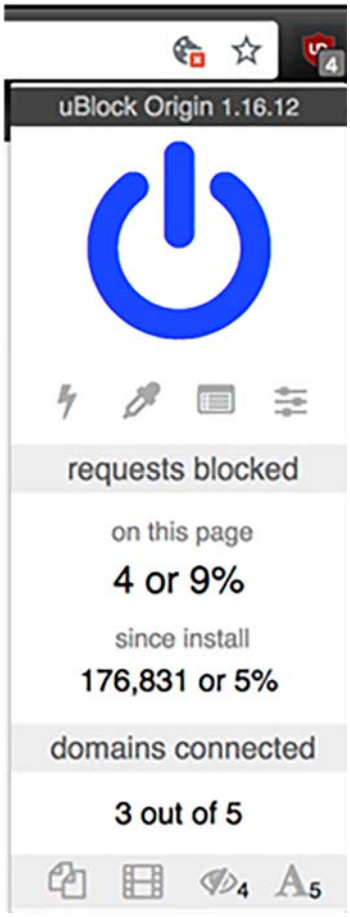


Cookie profiling is the only way for marketers to target potential customers and obtain a possible product purchase from them. By knowing a user's browsing habits, including sites visited, age, marital status, and political and religious affiliations, they can show him or her advertisements that are appealing, advertisements that he or she will care to patronize. This is a certain way for marketers to increase their profit by widening their customer base.

For a cookie guide please watch this video: https://www.youtube.com/watch?v=coWuhy3CjVE

More recently, consumers have been fighting back with a large growth in the number of 'ad-blocker' apps and extensions. These intercept http requests from your browser and filter out content being requested from known ad brokers or from an entirely different domain name. Not only does this reduce tracking, it speeds up the time taken to display the page.

There is a down-side though; many free-to-view websites rely on advertising income to make a profit so there is a fear that increased use of blocking technology will reduce the amount of free content available on the web; more and more sites will require you to subscribe instead.



uBlock Origin extension for Chrome —a popular ad blocker

Activity: Group discussion (10 min)

Discuss the issues around being tracked with some of your peers. Think about examples where you have been aware of being tracked, whether you use software to prevent this, and how worried you —and your friends are —about this. You should present your thoughts as a mind-map to your teacher/lecturer.

4.4 Denial of Service attacks

Learning objective

By the end of this section you will be able to:

- describe common faults caused by Denial of Service attacks;
- explain common symptoms, costs and effects of Denial of Service attacks;
- explain the motives behind Denial of Service attacks.

A Denial of Service (DOS) attack is when a website or a network is targeted, with the intention of making it unavailable to users. Denial of Service Attacks are almost always launched from outside an organisation, and are directed towards the services which the network is providing to the external users of that network. Denial of Service attacks may be designed to hold an organisation to ransom, put a competitor out of business, or be politically motivated.

You can read more about DoS attacks from the National Cyber Security Centre here: https://www.ncsc.gov.uk/guidance/understanding-denial-service-dos-attacks

4.4.1 Symptoms, costs and effects of an attack

There are a number of symptoms that a website or internet-connected resource could be being subjected to a Denial of Service attack:

- The web server may take a long time to respond to requests;
- The website could stop responding altogether;
- A low-graphics or temporary holding page may appear instead of the expected content;
- Database-driven content may take a long time to be fetched, or may fail;
- Individual elements of a page (such as CSS, images or JavaScript files) may fail to load;
- You may not be able to log in to online services and access data.

Effects of an attack

Ultimately the purpose of a DoS attack is to make it difficult for genuine users of a service to access it. This can be for many reasons (which are detailed in section 4.4.3).

A major effect of this is that businesses can have their income / sales disrupted as users are unable to interact with them. This can also have a bad effect on users too: we rely heavily on 'cloud-based' (i.e. web hosted) technology every day. Social media communications, email, online storage, educational resources (like Scholar!) can all be subjected to DoS attacks, causing major inconvenience for their users.

It is also worth knowing that a DoS attack can be used to distract IT personnel and resources while another crime is being committed such as an attempt to hack into the customer database!

Costs of an attack

Businesses suffering a DoS attack face two main costs:

- Lost revenue: Each time a service or online shop cannot be contacted by users or customers they are losing a sale! Many businesses carry out most —or sometimes all —of their business activity via the web, so this can have a huge impact on income.
- Staff costs: The labour costs of dealing with a DoS attack can be large. Specialist network engineers may be needed to recover crashed systems, put defences in place and try to stop an ongoing attack. The company may already employ these people, but will often rely on contracting in external help. This can be costly. There are also associated costs with increased workload and overtime for other staff who have to deal with a backlog of customer issues, complaints and communication that could not take place at the time of the DoS attack.

4.4.2 Types of attack

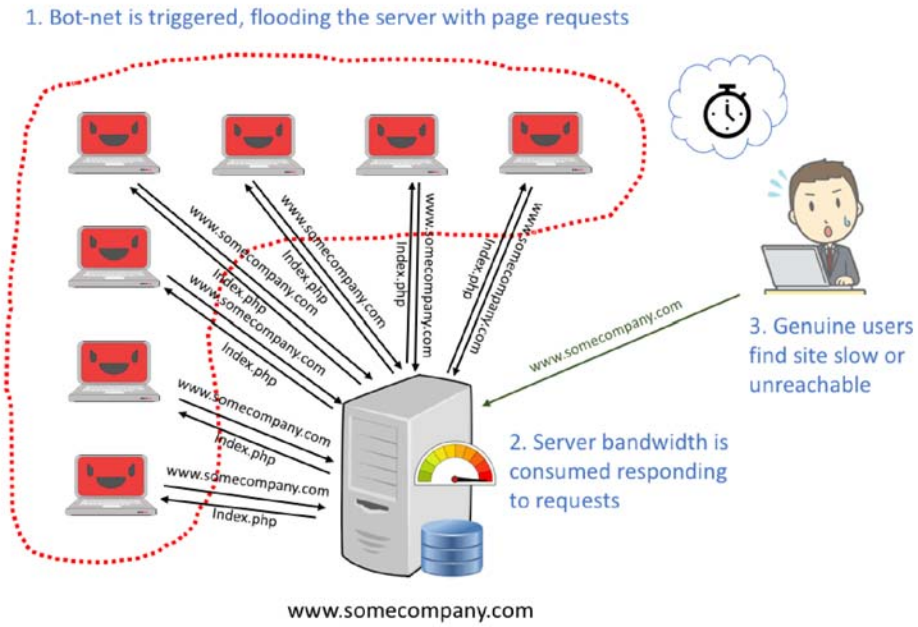
Bandwidth Consumption

The services provided by a network server depend on the bandwidth available to that server. Any attack which monopolises that bandwidth by consuming it unnecessarily can effectively deny users access to those services.

DoS attacks are often propagated by malware which install server software on unsuspecting users' machines. Port scanning software is used to identify the infected machines and then use them as a platform to mount repeated requests for pages. This gets around the fact that most websites will be hosted on servers with very high bandwidth which an individual computer could not swamp. Also, an individual computer could be easily blocked by the company's firewall!

These types of attack are known as a Distributed Denial of service attack (DDoS). A collection of infected machines is often referred to as a 'Bot-net'. Carrying out a DDoS attack is often straightforward —it is possible to buy access to bot-nets on the dark web —and while the server is being bombarded with spurious requests genuine visitors cannot get access to it.

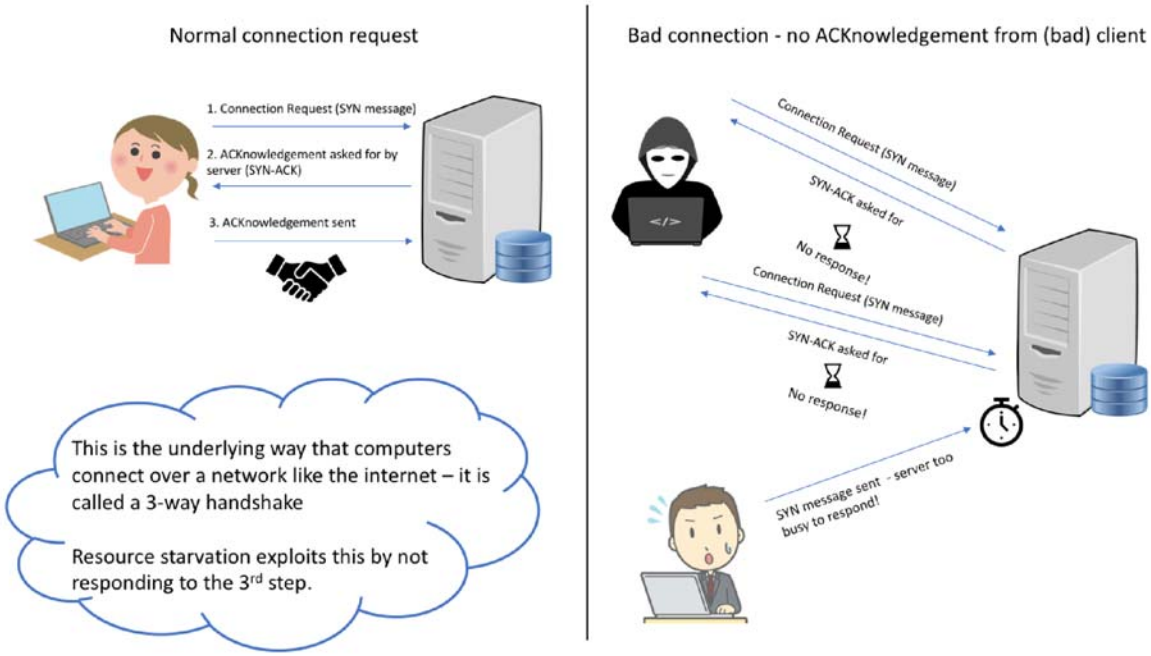
Most recently, hackers have exploited vulnerabilities in 'Internet-of-Things' devices such as lightbulbs and CCTV cameras to install bot-net software where it can run un-noticed by users.



Bot-net attack on a server; too many requests consume available bandwidth and slow down or stop genuine users from connecting.

Resource Starvation

Similar to bandwidth consumption, the server can have its resources 'tied up' by incomplete network connection requests. A common example is to 'ping' the server with a request to connect. The server will respond to this connection request and ask for an 'acknowledgement' from the client. If the client does not send the acknowledgement, the server will wait (sometimes for a long time) before dropping the connection request. This consumes RAM, processing time and network connections on the server again meaning that genuine users cannot connect.



An illustration of how resource starvation can be used to 'tie-up' a server with bad requests

In a similar vein, attackers can sometimes send processor-heavy requests across the web (for example a complex database search of an online store) in quick succession, consuming processor time and RAM.

Lastly, web services that allow users to upload content to their server can be subject to resource starvation by saturating the server with uploads; on a small server this may consume too much disk space and it will then fail to store genuine users' data.

Domain Name Service Attack

In a **DNS** attack, a large number of small DNS queries are sent from the attacker to DNS servers. These queries contain a spoofed IP address of the target server. The DNS servers respond to the small query with a large response which is routed to the target, causing congestion and consumption of bandwidth. This kind of attack can also cripple the DNS server. If attackers can control a DNS server then it is possible for them to redirect traffic from a legitimate site (eg a bank) to a fake site which harvests usernames and passwords.

4.4.3 Motives

There are a number of reasons for carrying out DoS attacks. Here are a few examples:

Curiosity / learning

Sometimes people carry out attacks just to see if it's possible. This is often done by people learning to hack, often without knowledge of the legal consequences of doing this. Sometimes the perpetrator may be aware of what they are doing and may be trying to establish a reputation in the hacking community.

Revenge Attacks

These have been carried out by ex-employees of companies to gain revenge for their dismissal, and even by disgruntled customers to protest their dissatisfaction.

Commercial competition

Online business is big business nowadays; corporations like Amazon, Google and Netflix make millions of pounds every minute that they are online. Even small businesses may lose out on crucial sales if customers cannot reach their website to make that purchase!

A business being subjected to a DOS attack firstly loses money, but it can also suffer reputational damage that can be difficult to recover from. Customers lose confidence —especially with repeated interruptions —and will often find alternatives. If you happen to be one of the alternatives, you have a lot to gain from your competitor going offline!

Political protest and 'hacktivism' Websites

Websites and services can be targeted for political or ideological reasons. Controversial people, parties and groups can be targeted to protest against their actions or beliefs. Large hacking groups like Anonymous have been known to employ this technique on a number of occasions, recently against resources known to be linked to the so-called 'Islamic State' terror group.

Cloaking

Sometimes hackers will launch a DoS attack to cover up an attack on other parts of a company's system that they are trying to break into. A company with limited resources may suspend other types of security monitoring and updates while their IT teams deal with the DoS attack, leaving an opportunity for hackers to exploit.

Cyber warfare

Increasingly, terrorist groups, military organisations and governments are waking up to the huge amount of disruption that cyber attacks like DoS can cause. The UK government considers this problem a 'tier 1 threat' to national security; that means it has the same scale of importance as a large military conflict or natural disaster.

Why is this such a problem? Much of our critical infrastructure is connected to the internet and relies on it to transfer data. All of the following services have the potential to be disrupted:

- Power Stations & the National Grid
- Traffic Management
- Air Traffic Control
- Railway signalling
- Government services
- Military communications
- Water treatment & supplies
- *and many more!*

Some of these areas have already been attacked successfully in other countries during wider conflicts.

Activity: Go online Go online 

Using the internet, find out about the following DoS attack examples. Create summary notes for each detailing the target(s) and try to explain what the motive was for each one.

- 'Mafiaboy' (2000)
- Estonia attack (2007)
- Project Chanology (2008)
- Operation Ababil (2012)
- Mirai botnets (2016 onwards)

4.5 Encryption

Learning objective

By the end of this section you will be able to:

- describe how public-key encryption ensures secure transmission of data;
- describe how digital certificates and digital signatures work.

4.5.1 Encryption overview

Encryption means that before information is sent or stored electronically, (for example in an email), it is scrambled using a mathematical process which turns it into something that looks like nonsense. This means that if anyone steals the information it will be meaningless to them. It will look like gobbledygook. Encryption is always a trade-off between security and convenience: it takes time and processing power to carry out encryption and decryption, often with specialist software needing to be installed.

When the information needs to be accessed by someone that has permission it is decrypted. The person who has received the encrypted email will have the key to the code and be able to decrypt the email. This means that it becomes readable again.

Encryption can be used on files that are stored on a computer or a backing storage device. Information that is in long term storage may have encryption applied to it to prevent it being accessed by hackers. Laptops and backing storage devices that contain sensitive information can benefit from being encrypted. There have been several occasions where government officials have lost laptops that have contained information that they do not wish to become publically available. If the information is encrypted, even if the laptop is stolen, the contents should remain private. It is now regarded as best practice for any portable devices containing personal or sensitive data to be encrypted. This is one step an organisation may take to meet their obligations under the **Data Protection Act** .

The military make use of encryption to protect their sensitive files and emails. In fact, one of the world's earliest computers was used to decipher the Enigma codes used during World War 2. Alan Turing used decoders called bombes to test all 17,576 possible Enigma ciphers until the coded messages were cracked.

Encryption does not prevent hacking but it means that when information is intercepted it cannot be read and is therefore worthless.

What is encryption?

Since the earliest days, people have invented various ways to send coded information to maintain secrecy. One of the simplest ways of doing this was the Caesar cipher. This is a simple technique - reputed to be invented by Julius Caesar to protect military commandments - whereby you 'shift' the letters of the alphabet by a fixed number. So, for example, if you employ a shift of 2, A becomes C, B becomes D, and so on.

Because of the simplicity of this system it offers little protection in reality, even without the power of a computer most Caesar Ciphers can be worked out with just a little knowledge of language. Picking on an often-used word or letter combination (The, Qu, ing,) will often reveal the offset quickly.

Activity: Crack the code! (5 min)

See if you can work out the hidden message here.

Ciphertext: L DP OHDUQLQJ DOO DERXW HQFUBSWLRQ ZLWK VFKRODU

Note: There are only 2 words in English with one letter!

To get around this problem, you need to scramble data using a more 'randomised' pattern, and one that changes the output in a less predictable way so that the same letter may be encoded into different 'ciphertext' letters. Perhaps the most famous example of trying to achieve this is the aforementioned 'enigma' machine of WWII, which used 3 dials (later 4) which rotated in a set pattern after every keypress. This caused a real problem for those trying to decode the messages, hence the development of early computers: instead of trying to figure out a simple substitution, you have to potentially test every possible scrambling permutation of the machine.

Modern computers now employ a much more sophisticated 'scrambling' system called key-based encryption, to protect against the power of other computers being able to try out millions of combinations every second: a virtual arms race!

4.5.2 Public and private keys

There are two types of key-based encryption: symmetric key and public key.

When using symmetric key encryption the key for encrypting and decrypting the information is the same. This key must be agreed between both parties before the transfer of information begins. Of course, the big weakness of symmetric encryption comes in trying to transmit the encryption key without it being intercepted! To get around this problem, asymmetric —or 'public key' encryption was developed.

Public key encryption (sometimes called asymmetric encryption) is a complex mathematical process involving the generation of two keys: a public key and a private key. Both keys are mathematically linked using very large prime numbers. Both keys work as a pair:

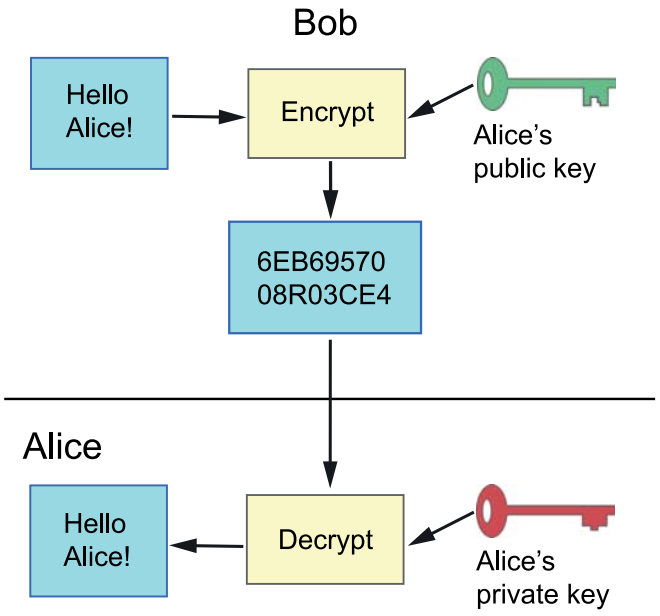
- The private key can encrypt data that can only be decrypted with the corresponding public key, and —going the other way —can decrypt data that has been encrypted by the corresponding public key.
- The public key can encrypt data that can then only be decrypted with the corresponding private key. The public key can also decrypt data that has been encrypted with the private key. Which way around this happens depends on our purpose.

Here is an example of how SSL - a popular encryption system for secure websites —works:

1. Your browser will be sent the website's public key —the private key remains on the server, so is still secure and cannot be intercepted.
2. Your browser uses the public key to encrypt the data you are sending (your credit card number?).
3. The data is sent back to the server —even if someone has intercepted the public key and your message they are still no further forward.
4. Once back at the server, the private key is used to decrypt the message.

In the next section, we will look at digital signatures, which use the two keys the other way around (the private key encrypts the data).

Figure 4.2: The encryption and decryption process



Key based encryption used by a typical secure browser session can use a scrambling key of some $1.6x10^{77}$ combinations —enough even to keep a supercomputer churning away until the end of time!

There is a good summary of the two types of encryption here: http://youtu.be/ERp8420ucGs

Quiz: Encryption (15 min) Go online

Q11: Explain what is meant by encryption?

. . . . . .

Q12: What are the benefits of encryption?

. . . . . .

Q13: Explain the difference between symmetric and public key encryption.

4.5.3 Digital certificates and signatures

Learning objective

By the end of this section you will be able to:

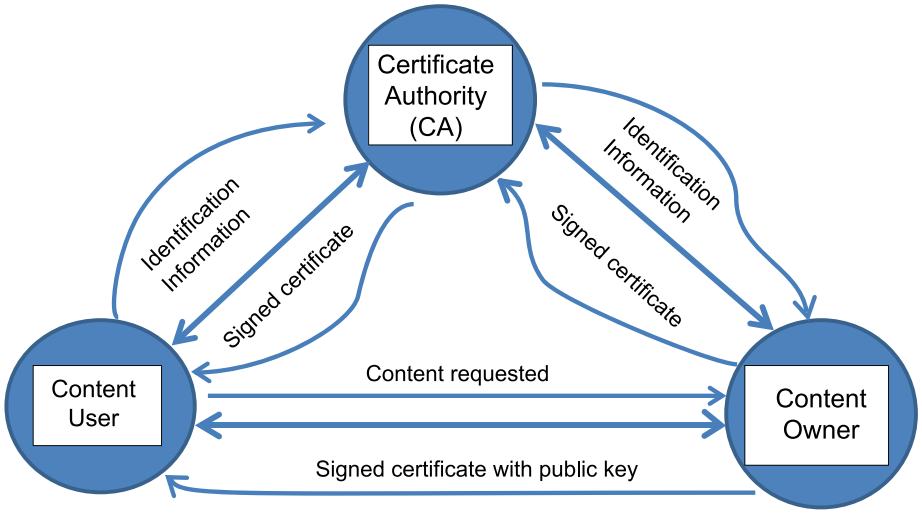
- describe a digital certificate;
- state the purpose of a digital signature.

A digital certificate can be known as a digital key certificate, public key certificate or an identity certificate, but they all refer to the same product. A digital certificate is an electronic document that

contains a digital signature, which confirms the name and identity of a person or organisation. The digital certificate uses a public key to bind the digital signature and identity together.

A public key, or public key infrastructure (PKI), is a scheme that allows companies and individuals to state that the identity information and the public key belong together.

Figure 4.3: Digital certificate process



A digital certificate becomes the equivalent of an electronic passport. It allows individuals or companies to feel secure in exchanging information as they each know the identity of the other party. A digital certificate is exceptionally hard to forge and can be trusted as it will have been issued by a trusted agency.

A digital certificate will contain the name of the certificate holder, serial number, expiry dates, public key for encrypting messages and the digital signature of the certificate issuing authority (CA).

Digital signatures

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document has not been tampered with. Digital signatures are easily transportable, cannot be forged by someone else, and can be automatically time stamped.

Digital signatures are supported by a wide variety of software packages used by business. This ensures that legally important messages arrive intact, are timestamped and can be trusted to be genuinely from the sender.

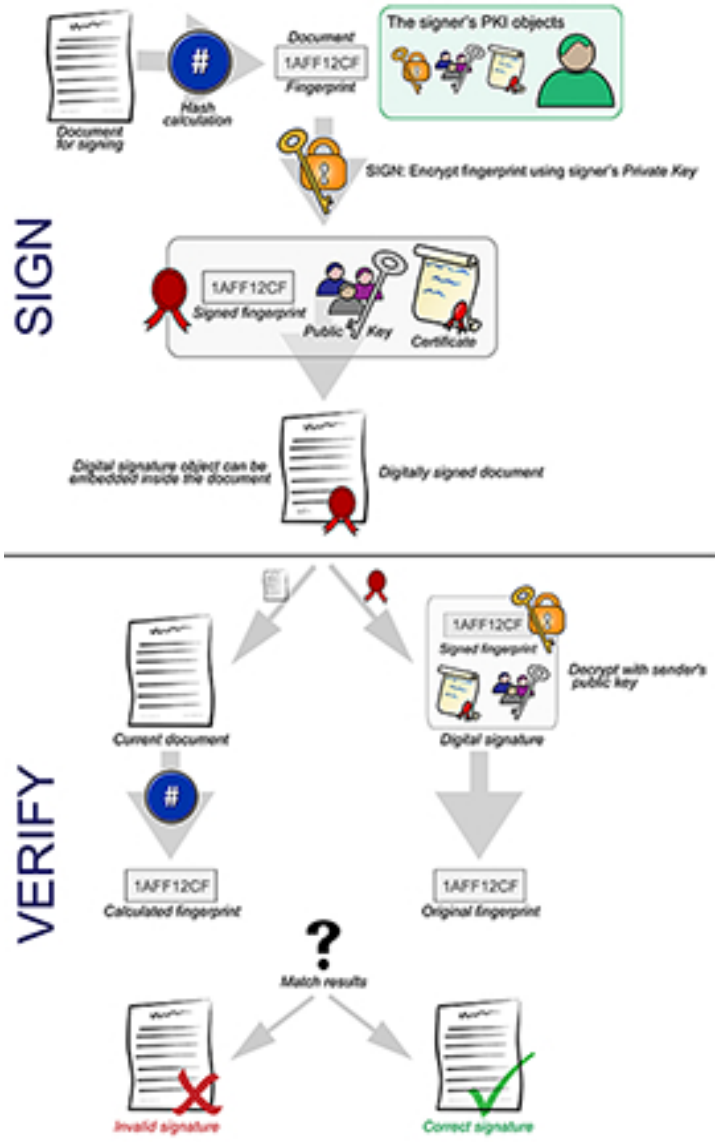
For example, assume that you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

- You copy-and-paste the contract into an e-mail.
- Using special software, you generate a message hash (mathematical summary) of the contract.
- You then use a private key that you have previously obtained from a public-private key authority (along with your digital certificate and public key) to encrypt the hash.
- The encrypted hash becomes your digital signature of the message. (Note that it will be

different each time you send a message as the hash is generated from the message contents directly). This is then attached to the original message and sent to the lawyer.

At the other end, your lawyer receives the message.

- To make sure it's intact and from you, your lawyer's software makes a hash of the received message.
- Your lawyer's software then uses your public key to decrypt the original hash that was calculated before the message was sent.
- If the decrypted hash value matches the hash value that the lawyer has calculated, then it is unchanged from when the document was signed. Note that this process also proves the original sender is the author (you): only you would have access to your private key, so if your - linked - public key can decrypt the hash value, only you could possibly have sent it. (This is an important legal point called repudiation —it basically means you can't later deny you sent the message with those contents).



Quiz: Digital certificates & signatures (25 min) Go online

Q14: What is a digital certificate?

. . . . . .

Q15: What is the purpose of a digital certificate?

. . . . . .

Q16: Who can make use of digital certificates?

. . . . . .

Q17: What is a digital signature?

. . . . . .

Q18: What is the purpose of a digital signature?

4.6 Learning points

Summary

- The Computer Misuse Act (1990) defines three activities that are illegal in the UK:
  - Unauthorised Access to Computer Material;
  - Unauthorised Access with intent to commit a further offence;
  - Unauthorised impairment/modification of programs or data.
- The Computer Misuse Act (1990) effectively outlaws hacking and the spreading of viruses (and some other types of malware program).
- Tracking cookies are placed by ad-brokers to keep track of your web browsing across multiple pages that use their service, building a profile about your interests and lifestyle to target adverts at you.
- Tracking cookies can be blocked by ad-blocking extensions and apps, but many websites rely on advertising revenue for income.
- A Denial of Service attack is where an attacker tries to stop people accessing a web-based service.
- Users will experience slow responses from attacked websites or may be unable to access it altogether.
- Denial of Service attacks can be based around bandwidth consumption (flooding the site with traffic), resource starvation (tying up key network or server resources), or by attacking DNS servers that are used to convert URLs into IP addresses.
- Denial of Service attacks can cost targeted sites revenue and loss of reputation.
- Motives for carrying out a Denial of Service attack include: curiosity, revenge, political reasons, commercial competition and cyber warfare.
- Symmetric key encryption uses the same key for both encryption and decryption. This has to be agreed securely before use.
- Public key encryption means that the encryption key is public and available for anyone to use to encrypt data. Only the private key can decrypt data encrypted by the public key.
- A digital certificate is an electronic document that contains an electronic signature and is used to confirm the identity of a person or organisation.
- A digital signature is an electronic signature that can be used to authenticate the identity of someone sending you information. It also confirms the integrity of the document.

4.7 End of topic test

End of topic 4 test Go online

Q19: Which of the following is a crime under the Computer Misuse Act (1990)?

a) Stealing a colleague's password and logging into a workplace computer with their details.
b) Holding personal data in an insecure manner.
c) Copying music from the internet.
d) Sending Spam emails.

. . . . . .

Q20: A tracking cookie stores:

a) Details of your age, gender and location.
b) Food and dietary preferences.
c) A unique identifier for an ad-broker agency.
d) All of your browsing history.

. . . . . .

Q21: Users of a website undergoing a Denial of Service attack may experience which symptoms?

a) Faster page load times than usual.
b) Inability to access the website, or very slow load times.
c) Premium features being accessible for free.
d) Hacking attacks on their computer.

. . . . . .

Q22: Which type of Denial of Service attack uses a botnet to generate a huge increase in network traffic directed at a website?

a) Bandwidth consumption
b) DNS attack
c) Resource starvation
d) Ping of Death

. . . . . .

Q23: When using public key encryption to communicate with a secure web server, how is the public key used?

a) The public key is used to decrypt data by the web server.
b) The public key is used to transfer the private key to the web browser.
c) The public key is not used; only the private key is needed.
d) The public key is used to encrypt data by the web browser.

. . . . . .

Q24: When receiving a document containing a digital signature, the receiver uses what key(s) to ensure the document is genuine?

a) The sender's private key
b) The sender's public key
c) Both public and private keys
d) Neither keys —a hash value is sent instead

Topic 5

End of unit 2 test

End of unit 2 test Go online

Q1: What is the largest positive decimal number which can be stored using 8 bit two's complement notation?

a) 256
b) 257
c) 127
d) 128

. . . . . .

Q2: Convert -35 into 8-bit two's complement notation.

a) 1101 1101
b) 1101 1100
c) 0010 0011
d) 1101 1110

. . . . . .

Q3: How many colours can be represented if the bit depth of an image is 32 bits?

a) 65,536
b) 16,777,216
c) 4,294,967,296
d) 1,099,511,627,776

. . . . . .

Q4: Increasing the number of bits representing the mantissa in a floating point number:

a) increases the range of numbers which can be represented.
b) increases the accuracy of the numbers represented.
c) decreases the accuracy of the numbers represented.
d) decreases the range of numbers which can be represented.

. . . . . .

Q5: Increasing the number of bits representing the exponent in a floating point number:

a) increases the range of numbers which can be represented.
b) increases the accuracy of the numbers represented.
c) decreases the accuracy of the numbers represented.
d) decreases the range of numbers which can be represented.

. . . . . .

Q6: Decreasing the number of objects in a vector graphic image:

a) increases the file size.
b) decreases the file size.
c) increases the resolution of the image.
d) decreases the resolution of the image.

. . . . . .

Q7: How will the contents of an array of integers be stored in memory?

a) Using floating point notation.
b) Using two's complement notation.
c) As binary numbers.
d) As a binary file.

. . . . . .

Q8: A computer uses a floating point system consisting of 1 bit for the sign bit, 12 bits for the mantissa and 7 bits for the exponent. What would the fractional number +1101.00001 be stored as?

a) 1 000110100001 0000100
b) 0 000110100001 0000100
c) 1 0000100 000110100001
d) 0 110100001000 0000100

. . . . . .

Q9: An advantage of UniCode over ASCII is:

a) It takes less storage space up.
b) It can represent all major world languages.
c) Old computers cannot read it, forcing people to upgrade.
d) It can be encrypted, unlike ASCII.

. . . . . .

Q10: Registers are:

a) areas on a hard disk.
b) memory locations in RAM.
c) memory locations in the processor.
d) memory locations in the cache.

. . . . . .

Q11: The number of lines in the data bus determines:

a) the word size of the processor.
b) the maximum addressable memory.
c) the maximum clock speed.
d) the minimum number of instructions processed per cycle.

. . . . . .

Q12: The number of lines in the address bus determines:

a) the maximum word size of the processor.
b) the maximum clock speed.
c) the number of instructions processed per cycle.
d) the maximum amount of addressable memory.

. . . . . .

Q13: After an instruction has been fetched from the RAM and transferred into the Instruction Register the next step is to?

a) Execute the instruction in the A.L.U.
b) Fetch the next instruction.
c) Execute the instruction in the registers.
d) Decode the instruction in the Control Unit.

. . . . . .

Q14: Which two factors below will affect the performance of a computer processor?

a) Amount of installed RAM, Clock Speed.
b) Upgrading to an SSD, Battery Capacity.
c) Clock Speed, Number of Cores.
d) Type of cooling, amount of RAM installed.

. . . . . .

Q15: What is cache memory?

a) Spare RAM for when the Operating System needs extra.
b) A small, fast area of memory located between RAM and the processor.
c) Another name for fast ROM chips.
d) Extra registers on high-powered processors.

. . . . . .

Q16: Which of the following computer technologies can benefit the environment? You may choose more than 1 answer.

- Smart heating systems for your home.
- Multi-core processors.
- Traffic management systems.
- Increased RAM capacities.

. . . . . .

Q17: Which of the following intelligent systems would not reduce the environmental impact of a car?

a) ABS braking system.
b) Start/stop technology.
c) Engine management systems.
d) 'Eco' mode.

. . . . . .

Q18: How does a sat-nav app help to reduce the impact of your driving on the environment?

a) It makes you drive faster so you spend less time on the road.
b) It tells you how long you will be queueing for.
c) It will only work with modern vehicles so encourages people to buy more efficient cars.
d) It can use real-time traffic information to plan the most efficient route and cuts down on congestion as a result.

. . . . . .

Q19: Which law makes spreading a virus illegal?

a) Computer Misuse Act
b) Copyright, Designs and Patents Act (Plagiarism)
c) Communication Act
d) Regulation of Investigatory Powers Act

. . . . . .

Q20: What is the main concern web users have about tracking cookies?

a) They allow advertising companies to build a detailed profile of our digital lives.
b) They take up a lot of space on the hard disk.
c) They can be used by the Tax office to detect undeclared income.
d) They will only allow you to buy from selected companies online.

. . . . . .

Q21: What is meant by a Denial of Service Attack

a) When a company refuses to serve a known hacker.
b) When an attacker uses techniques to try and stop genuine users from accessing a website or online service.
c) When you complain about the availability of an online system.
d) When you are refused entry to a bar by overly-aggressive door staff.

. . . . . .

Q22: Alice wants you to send her an encrypted message so gives you her public key. How can this message be decrypted?

a) By using Alice's public key again.
b) By using a symmetric key.
c) By using Alice's private key.
d) It cannot be decrypted as you only used the public key.

. . . . . .

Q23: Which of the following is true about a digital signature?

a) It can verify both the sender's identity and the integrity of the original message.
b) It can only verify the sender's identity —someone may still have tampered with the message.
c) It can only verify the message —anyone could have sent it.
d) It cannot verify anything as it is just a bitmap image of your real signature.

Answers to questions and activities

Topic 1: Data representation

Quiz: Revision (page 3)

Q1: a) Computers only understand machine code

Q2: b) High level languages are often written to solve particular types of problem

Q3: Bitmaps are stored as a 2-dimensional array of dots called pixels. Each pixel is represented by a binary number representing its colour

Q4: b) Polygon

Quiz: Using binary code to represent and store numbers (page 4)

Q5: Arithmetically things would have been simpler for humans if we had evolved with six digits on each hand rather than five, because this would have probably meant that we would have used a base 12 number system instead of base 10. 10 is not easily divisible by anything other than 2 and 5 making fractions like a third and two thirds an inconvenience. We are stuck with the decimal system however and are unlikely to be changing it in the near future due to the fact that we have 5 digits on each hand.

Example of binary to denary conversion (page 5)

Q6: 118

Q7: 54

Q8: 986

Q9: 223

Q10: 160

Q11: 3276

Example of denary to binary conversion (page 6)

Q12: 10000110

Q13: 10010100

Q14: 11101

Q15: 10010

Q16: 1001111

Q17: 100010001

Answers from page 9.

Q18: b) 0..255

Q19: c) 0..4095

Q20: a) $0..2^n-1$

Quiz: Two's complement (page 11)

Q21: the number is negative because its most significant (leftmost) bit is a 1 and it is odd because there is a 1 at the end whose value is 1.

Questions: Two's complete (page 13)

Q22: b) -32 to +31

Q23: d) -512 to +511

Questions: Floating points (page 16)

Q24: = $0.11010001 \times 2^4 = 1101.0001$

Q25: = $0.11000000 \times 2^{-4} = 0.000011$

Q26: = $-0.10101111 \times 2^6 = -101011.11$

Q27: 0 1111001 0010

Q28: 1 1100000 1011

Q29: 0 1101001 0110

Answers from page 18.

Q30:

- 16 bits allows 65,536 characters.
- 32 bits allows 4,294,967,296 characters!

Bitmap and vector format (page 23)

Q31:

BITMAP FORMAT	VECTOR FORMAT
Suitable for natural, realistic images	**Suitable for graphic, unrealistic images, designs and drawings**
Advantages: Images can be very realistic (e.g. digital photograph). Pixel level editing is allowed —allowing effects such as spray paint, blur, effects and so on. Same appearance in all systems, regardless of hardware or software.	Advantages: Can be scaled to large sizes, keeping original quality. Individual objects can be edited, allowing an object to be altered without affecting the rest of the image. Are easily converted to bitmap formats. File sizes are relatively small. Size of image can be increased keeping quality and file size the same.
Disadvantages: Scaling causes pixilation. Only the image as a whole can be edited. Are very difficult to convert to vector formats, with unpredictable results. File sizes can be large. Increasing the image size needs re-sampling and increases the file size.	Disadvantages: Difficult to create realistic images. Only individual objects can be edited (it is sometimes impossible to edit only part of the object). Dependent on output hardware or software for appearance & quality.

End of topic 1 test (page 25)

Q32: d) 1011 0111

Q33: c) -2048 to +2047

Q34: c) Accuracy increases, range decreases

Q35: b) 1 11010100 0000011

Q36: d) 65536

Q37: c) 23.9 MB

Q38: a) increases the file size

Topic 2: Computer structure

Quiz: Revision (page 29)

Q1: d) ALU, Control Unit, Registers

Q2: The data bus is a bi-directional set of wires that transfer data between the processor and memory.

Q3: a) Unique binary numbers

Activity: Read and write operations (page 31)

Q4:

1. Address of memory location to be read from is placed on Address register.
2. Memory location is identified.
3. Read line is activated.
4. Data is transferred to data register from memory location via data bus.

Q5:

1. Address of memory location to be written to is placed on Address register.
2. Memory location is identified.
3. Write line is activated.
4. Data is transferred from data register to memory location via data bus.

Quiz: Buses and their function (page 32)

Q6: b) carry a memory address from which data can be read or to which data can be written.

Q7: c) transfer data between memory and processor.

Q8: The address bus is used to identify a memory location in RAM, so there is no need for information to flow back from the memory to the processor over this bus.

Q9: 16777216

Q10: 32 Megabytes

Q11: Adding additional registers would speed up the fetch execute cycle because data could be moved between registers within the processor without having to access the cache.

Activity: Fetch-execute cycle (page 35)

Q12:

1. Transfer Program Counter to Memory Address Register
2. Increment the Program Counter
3. Activate Read line
4. Transfer instruction to Data Register and then to Control Unit
5. Decode Instruction
6. Execute Instruction

Quiz: Program counter (page 35)

Q13: An instruction in a program may be to load additional data from memory. The address of this data will need to be placed on the address bus using the address register, but the program counter is still needed to keep track of the address of the next instruction in the program.

End of topic 2 test (page 41)

Q14: c) Decode Instruction

Q15: a) Address of the next instruction

Q16: a) Increase the control bus width

Q17:

1. Registers
2. Cache
3. RAM
4. Hard Disk

Q18: b) Heat generation and power consumption increase in line with clock speed.

Topic 3: Environmental impact

Quiz: Revision (page 45)

Q1: c) Much of the electricity used by computers comes from non-renewable fossil fuels. Burning fossil fuels for electricity produces CO^2, a greenhouse gas.

Q2: a) Buying a more powerful processor.

Answers from page 46.

Q3: A computer system that has ability to perform tasks that would require intelligence if they were performed by a human. Intelligent systems display at least one form of behaviour that is similar to human intelligence.

Quiz: Heating systems (page 47)

Q4: The controller can use the GPS location from your smartphones to work out that no one is at home and turn down the heating automatically, or can be manually turned down remotely via an app.

Q5: You could set certain rooms that are not used frequently (e.g. a guest bedroom) to a lower temperature and boost the temperature briefly where needed in other rooms (e.g. increase the bathroom temperature in the morning).

Quiz: Traffic control (page 50)

Q6: c) Using up-to-date congestion information via an app to avoid queueing traffic.

Quiz: Car management systems (page 51)

Q7: Intelligent systems can also be used to increase safety when driving and carry out complex manoeuvres like reverse parking more reliably than a human.

End of topic 3 test (page 53)

Q8: b) A computer system that can make human-like decisions automatically based on input from sensors.

Q9: a) They can help to reduce the energy used to heat a home by monitoring usage patterns, weather and owner's location.

Q10: d) A 'Sport' mode to increase acceleration performance.

Topic 4: Security risks and precautions

Quiz: Revision (page 57)

Q1: b) Inform the UK Information Commissioner within 72 hours.

Q2: a) By only allowing data into your network on specific ports used by your software.

Q3: The scrambling of data using a complex process involving a 'key' value. It is unfeasible to reverse this process without knowing the key value.

Answers from page 58.

Q4: Expected Answer: The Computer Misuse Act (1990)

Activity: Computer Misuse Act (page 60)

Q5: c) Unauthorised acts with intent to impair operation of a computer

Q6: b) Unauthorised Access with intent to commit or facilitate commission of further offences

Q7: a) Unauthorised Access to Computer Material

Q8: a) Unauthorised Access to Computer Material

Q9: c) Unauthorised acts with intent to impair operation of a computer

Q10: b) Unauthorised Access with intent to commit or facilitate commission of further offences.

Activity: Crack the code! (page 70)

Expected answer

I am learning all about encryption with scholar.

Quiz: Encryption (page 71)

Q11: Encryption applies a code —called a key —to scramble information before it is transmitted in an attempt to protect it. If the data is intercepted it will be meaningless.

Q12: If data is intercepted it cannot be understood. A computer's backing storage can also be encrypted so that sensitive information is not vulnerable if the device is stolen.

Q13: In symmetric encryption both the key for encrypting and decrypting are the same and are agreed before information is transmitted. In public key encryption the encryption code is public and the decryption key is only available to the person receiving the information.

Quiz: Digital certificates & signatures (page 74)

Q14: A digital certificate is an electronic document that is used to confirm the identity of a person

or organisation.

Q15: The purpose of a digital certificate is to allow individuals and companies to feel secure in exchanging information as they are able to confirm each other's identity.

Q16: Anyone can make use of digital certificates.

Q17: A digital signature is an electronic signature that can be used to validate the identity of the person sending a message or document.

Q18: The purpose of a digital signature is to confirm and prove a person's identity.

End of topic 4 test (page 76)

Q19: a) Stealing a colleague's password and logging into a workplace computer with their details.

Q20: c) A unique identifier for an ad-broker agency.

Q21: b) Inability to access the website, or very slow load times.

Q22: a) Bandwidth consumption

Q23: d) The public key is used to encrypt data by the web browser.

Q24: b) The sender's public key

Topic 5: End of unit 2 test

End of unit 2 test (page 80)

Q1: c) 127

Q2: a) 1101 1101

Q3: c) 4,294,967,296

Q4: b) increases the accuracy of the numbers represented.

Q5: a) increases the range of numbers which can be represented.

Q6: b) decreases the file size.

Q7: b) Using two's complement notation.

Q8: d) 0 110100001000 0000100

Q9: b) It can represent all major world languages.

Q10: c) memory locations in the processor.

Q11: a) the word size of the processor.

Q12: d) the maximum amount of addressable memory.

Q13: d) Decode the instruction in the Control Unit.

Q14: c) Clock Speed, Number of Cores.

Q15: b) A small, fast area of memory located between RAM and the processor.

Q16:

- Smart heating systems for your home.
- Traffic management systems.

Q17: a) ABS braking system.

Q18: d) It can use real-time traffic information to plan the most efficient route and cuts down on congestion as a result.

Q19: a) Computer Misuse Act

Q20: a) They allow advertising companies to build a detailed profile of our digital lives.

Q21: b) When an attacker uses techniques to try and stop genuine users from accessing a website or online service.

Q22: c) By using Alice's private key.

Q23: a) It can verify both the sender's identity and the integrity of the original message.