Higher
Computing Science

Computer Systems

Pupil Notes

Name:_____

Contents

Data Representation

Integers: Positive Numbers

Numbers are represented in the computer system using binary

2^x	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

128 + 32 + 16 + 4 + 1 = 181

The column headings with a one beneath them are added together to give the number in denary.

Integers: Two's Complement

In two's complement, the **most significant bit** (largest column) is negative and all other columns are positive.

Example 1 (8 bit)

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

-128 + 32 + 16 + 4 + 1 = -75

-128	64	32	16	8	4	2	1	
1	0	1	1	0	0	1	1	**-77**
1	0	0	0	0	0	1	1	**-125**
1	1	1	1	1	1	1	1	**-1**

In two's complement, the largest column value is negative and all other columns are positive.

When the most significant bit is a 1, the number is negative. When it is a 0 the number is positive. For this reason it is called the **sign bit.**

Example 2 (5 bit)

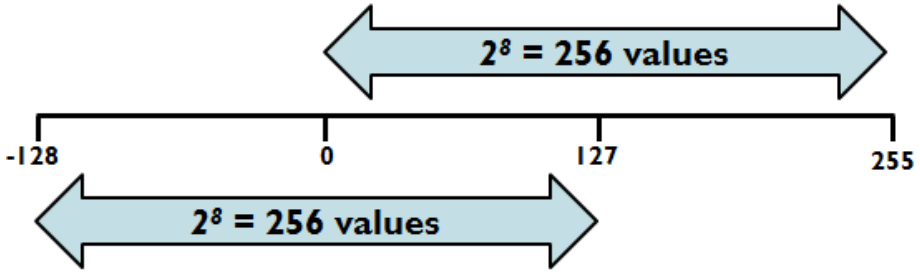
-16	8	4	2	1
1	0	1	0	1

-16 + 4 = -12

-16	8	4	2	1	
1	1	1	0	1	-3
0	0	1	1	1	7
1	1	1	1	1	-1

Range of Integers

An 8 bit number can represent the numbers from **00000000** to **11111111** (0 to 255)



An 8 bit two's complement number can represent the numbers from **10000000** to **01111111** (-128 to 127)

Reading Review 1

Having read pages 5 – 6, answer the questions below.

1. Convert the following negative decimal numbers into binary using **8 bits**.

a)- 5

b) -111

c) -74

d) -16

e) -52

2. Convert the following **negative** 8 bit binary numbers into decimal

a) 10111010

b) 10010011

c) 11100110

d) 10101010

e) 11110000

Real Numbers

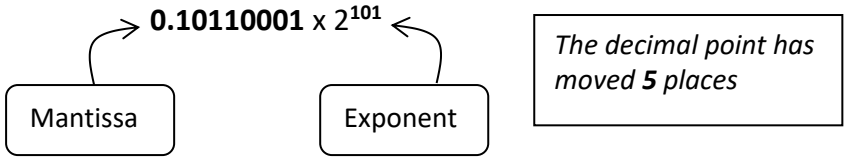
Real Numbers are numbers that contain a decimal point – they are stored using **floating point notation**.

Example 1

The computer would store the real number:

10110.001

In two parts:

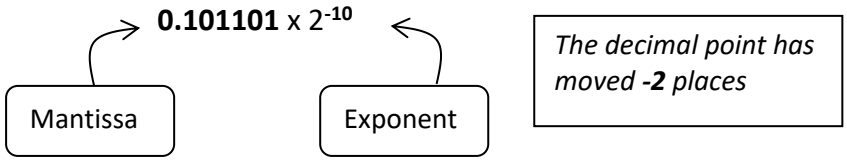


Example 2

The computer would store the real number:

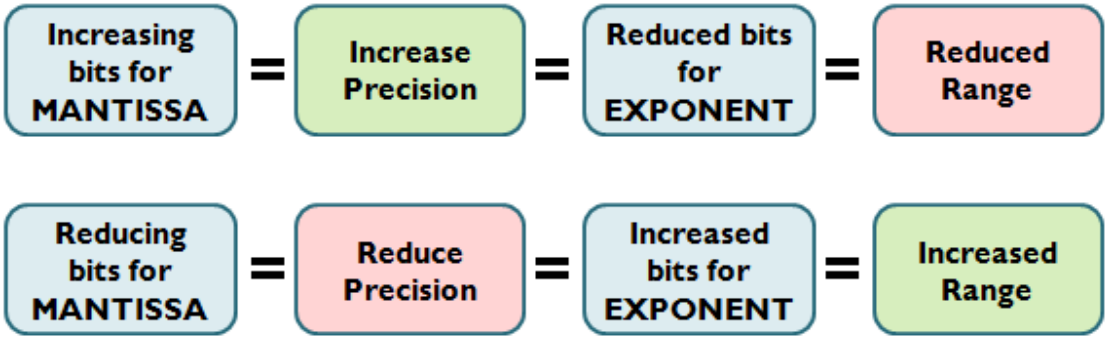
0.00101101

In two parts:



The number of bits allocated to the **mantissa** affects the **precision** of the number

The number of bits allocated to the **exponent** affects the **range** of numbers



If 16 bits are allocated to a floating point number, they could be allocated as:

11111111 x 2 **11111111**

The allocation of bits could be changed:

Increased range, reduced precision	**1111** x 2 **111111111111**	**111111111111 x 2** **1111**	*Reduced range, increased precision*

Reading Review 2

Having read pages 8 – 9, answer the questions below.

1. Real numbers are stored in two parts.

a) State the name each part.

_____

_____

b) For each part, state whether it affects the range or precision of the number

_____

_____

2. A programming language uses 32 bits to represent a real number such as 0.000000034. 8 bits are used for the exponent and 24 bits are used for the mantissa.

a) State the effect on range and precision if this allocation was changed to 16 bits each for both exponent and mantissa.

_____

_____

_____

b) Explain the additional consideration required to store the number -0.000000034

_____

_____

_____

Characters (Text)

The computer can only represent data using binary (1 or 0). To represent characters, they have to be converted into numbers which can then be stored as binary values.

Example:

A = 65 01000001

B = 66 01000010

C = 67 01000011

Text can be encoded like this using:

- **ASCII**
- **Unicode**

ASCII

ASCII (American Standard Code for Information Interchange) is a standard format for encoding text.

ASCII uses 8 bits (1 byte) to store each character meaning a total of 256 characters can be represented.

> *The word "Computing" has 9 characters, so an ASCII file containing only this word would take up 9 bytes of storage*

256 characters is not enough to store the symbols from all the different languages and fonts we use.

This is a major limitation of the ASCII format.

ASCII Table

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Unicode

Unicode deals with the limitation of ASCII by using **16 bits** (2 bytes) to **store** each character.

This means a total of 65,536 characters can be represented.

> *The word "Computing" has 9 characters, so a Unicode file containing only this word would take up 18 bytes of storage*

Although Unicode overcomes the limitations of ASCII, its files requires double the storage capacity.

Reading Review 3

Having read pages 11 – 12, answer the questions below.

1. Explain, in detail, how it is possible to represent characters using binary.

_____
_____
_____
_____
_____
_____

2. Describe one advantage and one disadvantage of using Unicode instead of ASCII to represent characters.

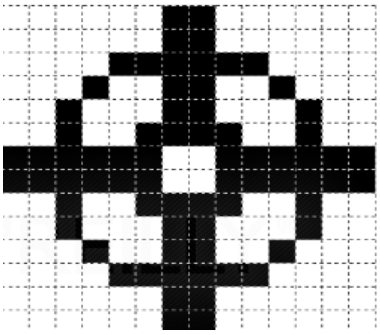
Advantage:

_____
_____
_____

Disadvantage:

_____
_____
_____

Graphics: Bit-mapped

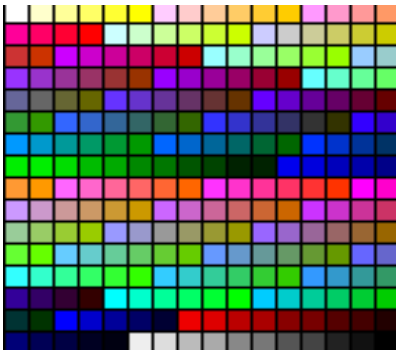


Black and white images are represented by a 2D array of pixels.

Each pixel is represented by a **1 bit** binary number: **1** for black, **0** for white.

Count the number of pixels to determine the **resolution.**

Colour images have to use more than 1 bit per pixel in order to represent more than 2 colours.



Bits per pixel		Colours Possible
1	2^1	2
2	2^2	4
3	2^3	8
8	2^8	256
16	2^{16}	65536
24 (*true colour*)	2^{24}	16,777,216

The number of bits per pixel is known as the **colour depth** and applies to **all** pixels in an image.

Vector Graphics

Vector graphics are used to create images made up of shapes and lines. They cannot be used to store detailed life-like images.

Vector graphics are stored as a detailed description of the **objects** and **attributes** used in the image.

Some objects and attributes for this shape are given below.

<**circle:** centre x, centre y, radius, line colour, fill colour>

<**rectangle:** x, y, width, height, line colour, fill colour>

<**line** x start, y start, x end, y end, line colour, line width>

Features of Vector Graphics

- Storing objects and attributes in a text file takes up very little space
- The more objects in an image, the larger the file size becomes.
- Images do not lose quality when they are scaled up.
- Shapes that make up an image remain separate and can be moved around individually

Vector Graphics v Bitmap Graphics

Vector Graphics	Bitmap Graphics
Objects can overlap other objects without rubbing out the one below	Objects that overlap **overwrite** the one below.
Increasing the size of objects does not alter the file size (size attribute is simply altered). Adding more objects increases file size.	Adding more details to the image does not affect the file size (same number of pixels used).
Object descriptions are saved as a series of attributes in a text file so **little storage space** required	Entire screen is saved (details of each pixel) so **file size is very large** regardless of the picture.
Object is **resolution independent**. Resolution it is created in has no effect on it at higher resolutions	**Resolution is fixed** when the picture is created. Bitmap will not take advantage of using a higher resolution later.
Individual pixels **cannot** be edited	Bitmap can be zoomed in so individual pixels **can** to be edited
Increasing the size of an object can be done **without** loss of quality. Attributes are simply re-written.	Increasing size of object will result in image becoming **pixelated.**

Reading Review 4

Having read pages 14 – 16, answer the questions below.

1. Describe two **advantages** of vector graphics over bitmap graphics.

_____

_____

_____

_____

_____

2. Describe two **disadvantages** of vector graphics over bitmap graphics.

_____

_____

_____

_____

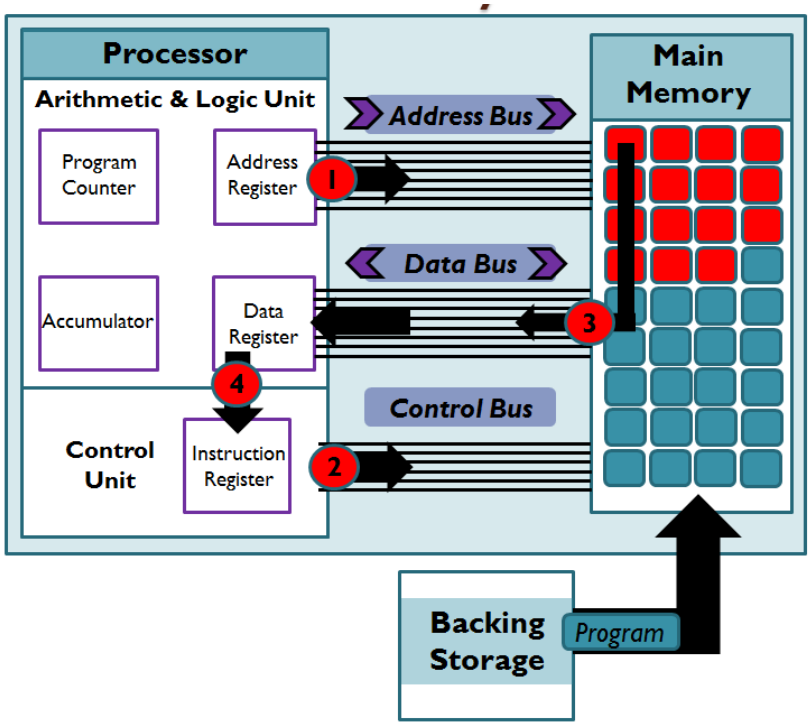
Computer Structure

Fetch-Execute Cycle

When a program is started, machine code **instructions** are **loaded** from backing storage into **main memory.** Each instruction for the program is located in a different **unique address location** in main memory

Fetch-Execute

The **fetch-execute cycle** is the process that retrieves the program instructions, one at a time, from RAM to the CPU where they are executed.



1. The address bus is set up (by the MAR) with the memory address location of next instruction to be fetched.

2. The **Read line** is activated on the **Control Bus** (to inform RAM that an instruction or data is to be transferred to the CPU).

3. **Instruction** at specified memory location is loaded onto the *Data Bus* which sends it to the Data Register.

4. Instruction is passed from Data Register to Instruction Register to be **decoded and executed.**

When the CPU needs to write data back to memory (e.g. an updated variable value) then a **memory write** operation must take place.

Memory Write

1. The address bus is set up (by the MAR) with the memory address location of next instruction to be fetched.

2. The data bus is set up (by the MDR) with the data to be stored in RAM.

3. The **Write line** is activated on the **Control Bus** (to inform RAM that an instruction or data is to be transferred from the CPU).

4. Data on the **data bus** is stored in the memory location specified by the **address bus**.

Reading Review 5

Having read page 18-19, answer the questions below.

1. With reference to buses and registers, write the main steps involved in the fetch-execute cycle.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

2. With reference to buses and registers, write the main steps involved a memory write operation.

_____

_____

_____

_____

_____

_____

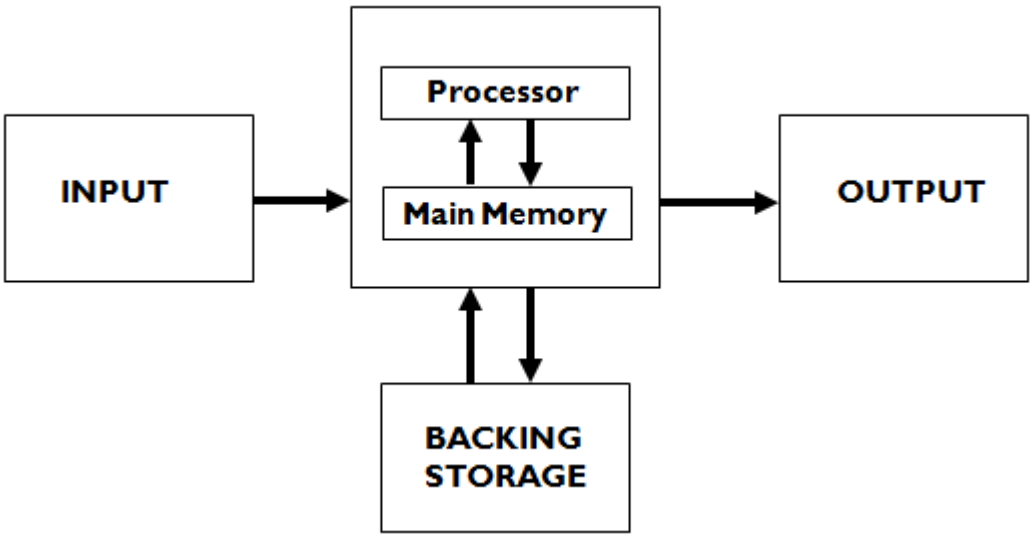
_____

_____

_____

_____

Computer System Block Diagram



- The **Processor** processes instructions stored in **main memory**
- The user communicates with the Processor via **input** devices
- The Processor communicates with the user via **output** devices
- **Backing storage** devices store programs and data permanently

Device Types

This model is shared by all computing devices such as:

Desktop Laptop Tablet Smartphone

Main Memory

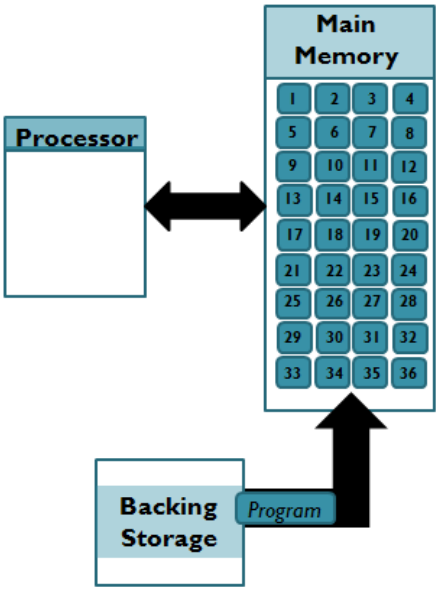
Main Memory consists of two types:

- **Random Access Memory (RAM)**
- **Read Only Memory (ROM)**

RAM

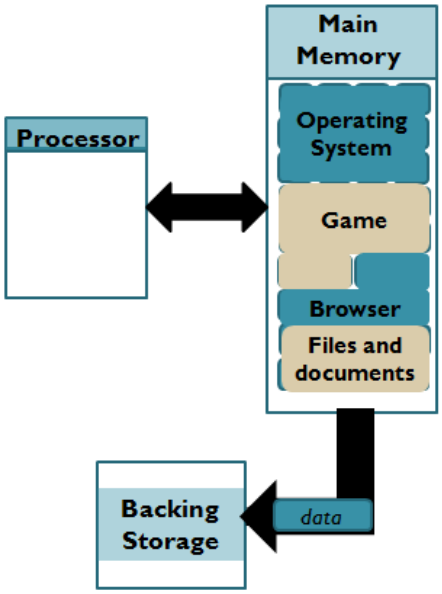
Each **storage location** has a unique address to identify it.

When a program is **loaded**, instructions are placed into these memory locations.



The more RAM installed in a computer, the more programs it can run simultaneously.

The operating system is a program and is therefore always using up a portion of the available memory.



Data stored in RAM **can be constantly changed** which allows different programs to be loaded.

When RAM is full no more programs can be loaded into memory

RAM is volatile so requires a constant power signal to retain its data.

Any data in RAM not saved to backing storage is **lost** when the computer is switched off

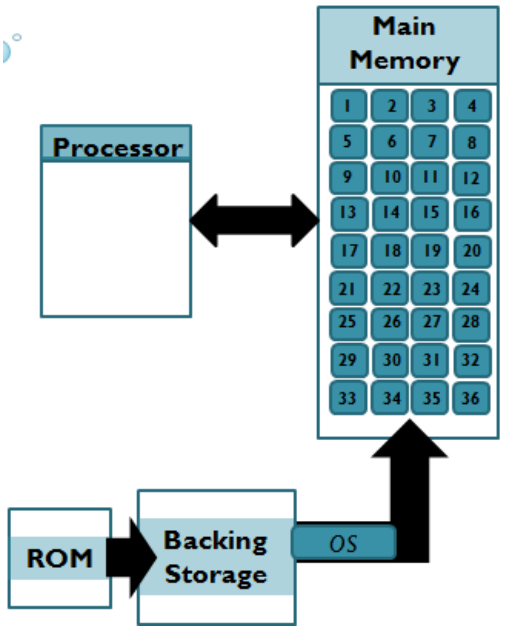
ROM

ROM is used to permanently store the files needed to **boot** (start) the computer system.

Data in ROM **cannot be changed**

ROM is non-volatile so it does not require power to retain its data.

The contents of ROM are not deleted when the computer is switched off.



Central Processing Unit

The CPU is the component of the computer system responsible for processing instructions.

It is the CPU that essentially makes a computer work. All computing devices contain a CPU.

Clock Speed

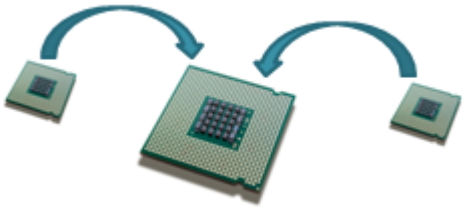
The CPU **clock** sends out a constant, steady pulse. **One** action is carried out by the processor on **each** clock pulse.

Clock speed (frequency) is measured in Hertz (Hz), meaning per second.	Typical computer is 3GHz That's 3000 million pulses per second

The faster the **clock speed**, the more instructions can be executed in a fixed time.

Processor Type

In the past, each CPU chip had a **single core**. This means that it contains one processor and can do **one** thing at a time.



Nowadays, CPU chips contain **dual core** (two cores) **or more** meaning they can do **more than one** thing simultaneously.

The more cores a CPU has, the more tasks it **can be** programmed to carry out at the same time, improving the performance of the computer.

If a piece of software isn't programmed to make use of these extra cores then they will not make any difference to the system performance.

Reading Review 6

Having read page 21-23, answer the questions below.

1. How are storage locations identified in RAM?

_____

_____

_____

2. Explain why RAM capacity is important to a computer system.

_____

_____

_____

3. When the computer is switched on, which program is always in RAM?

_____

4. Explain how the use of a multi-core processor would affect computer performance?

_____

_____

_____

_____

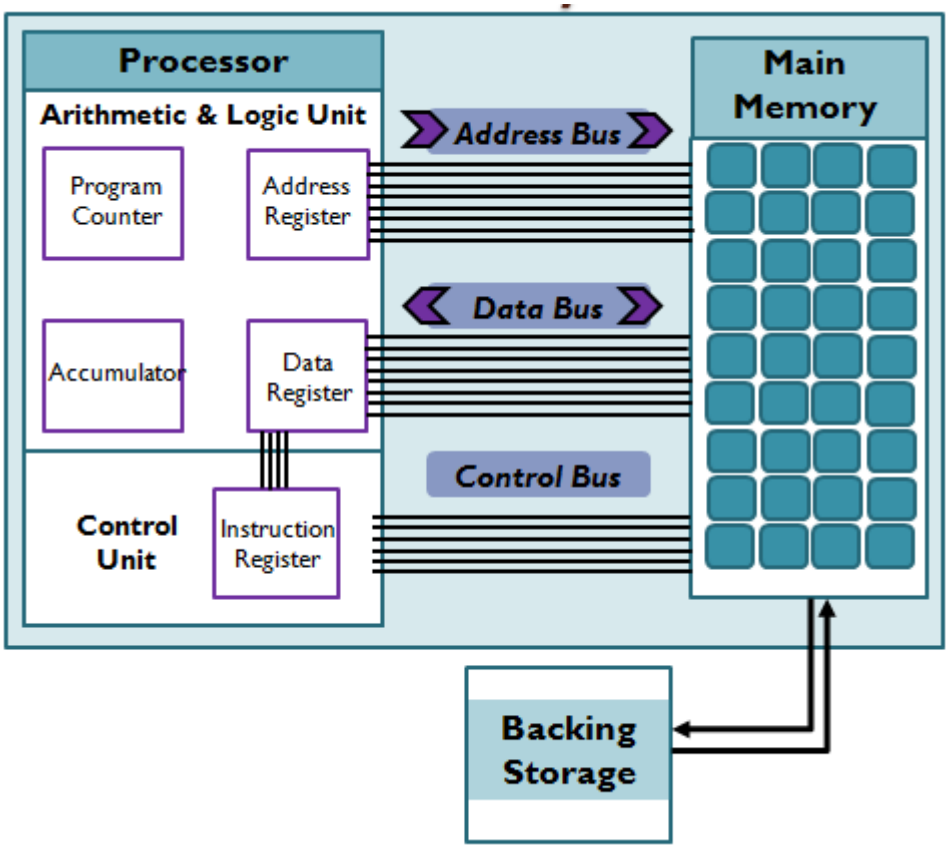
_____

_____

Parts of the CPU

The CPU consists of three main parts:

- **Arithmetic & Logic Unit**
- **Control Unit**
- **Registers**



Arithmetic & Logic Unit performs calculations and logical comparisons (used in evaluating conditions).

Control Unit provides timing and control signals which it uses to synchronise the fetching of instructions from memory

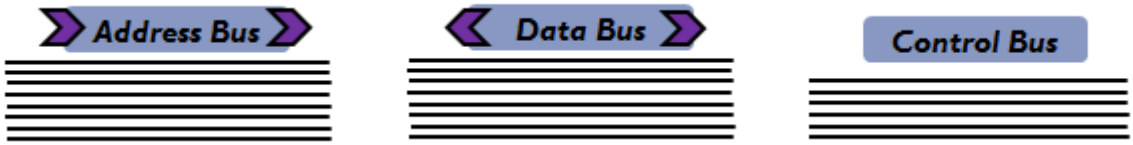
Registers are small, fast access, memory locations used to store **data**, **instructions** and **addresses** temporarily within the CPU

- **Program Counter (PC)** register stores the memory **address** of the **next instruction** to be fetched
- **Memory Address Register (MAR)** holds the **address** of the **current** memory location to be accessed
- **Memory Data Register (MDR)** holds data or instructions transferred between the CPU and memory
- **Accumulator** register holds temporary results of arithmetic and logic operations
- **Instruction Register (IR)** stores the current instruction being decoded and executed

Buses

Buses connect the CPU to main memory allowing them to communicate with each other.

The main CPU buses are:



Address Bus

The Address Bus is **unidirectional** meaning it only carries address information in **one direction**.

The Address Bus is used by the CPU to tell main memory which address location to open.

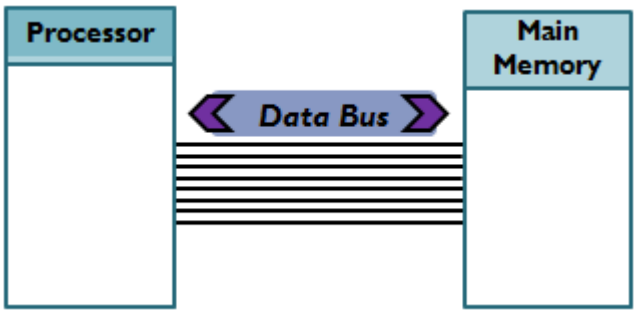
The number of lines on the address bus determines the number of possible address locations.

8 lines	= 2^{8}	= **256** addresses
16 lines	= 2^{16}	= **65536** addresses
24 lines	= 2^{24}	= **65536** addresses

Data Bus

The Data Bus is **bi-directional** meaning that it carries data in **both directions** between the CPU and memory.

As well as data, the Data Bus carries **instructions** from memory to the CPU where they are executed.



The number of lines on the data bus is equivalent to the size of each memory location. This is known as the **word size.**

8 lines	= **1** byte word size
16 lines	= **2** byte word size
24 lines	= **3** byte word size

Word size determines the number of bits that can be processed at any one time.

Increasing word size improves CPU performance by reducing the number of fetches to memory**.**

Reading Review 7

Having read page 25-27, answer the questions below.

1. State three things that can be stored in registers

_____

_____

2. By describing the purpose of the address bus, explain why it is sufficient for it to be unidirectional.

_____

_____

_____

_____

3. If a CPU has a 12 line address bus, what is the maximum number of addresses it can access?

_____

4. By describing the purpose of the data bus, explain why it is must be bi-directional.

_____

_____

_____

_____

5. If a CPU has a 16 line data bus, how many fetches to memory would it take to retrieve a 4 byte instruction?

_____

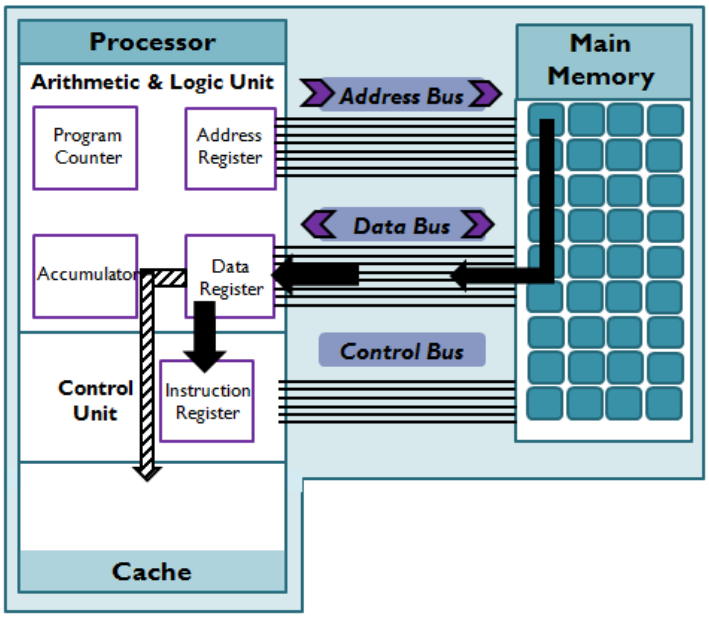
_____

Cache Memory

CPU overall performance is compromised by buses and main memory.

The CPU is much faster than these components so it has to wait on instructions and data being fetched.

The use of **cache memory**, located on the CPU, improves the CPU performance.



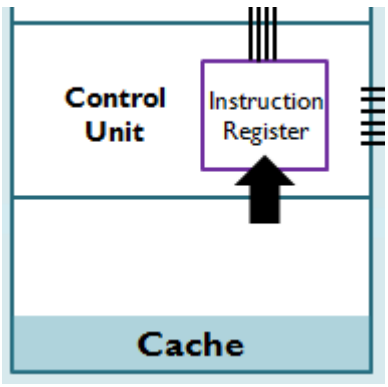
The CPU has to **wait** on the buses and Main Memory **fetching instructions** and data which is a **slow** process**.**

CPU **performance can be improved** by adding cache memory to the CPU

Cache memory is located on or close to the CPU itself which makes it **faster** to access data.

Cache stores copies of data from frequently used memory locations, or **reads ahead** to load the next instruction into cache

The CPU will firstly check cache for the instruction it needs saving it having to carry out a slow fetch to main memory.



Cache uses S-RAM chips which are **more expensive** (per MB) than main memory D-RAM chips, but **cache access time is faster.**

Increasing Clock Speed

- CPU can execute more instructions per second.
- Power consumption/heat increases so cooling is more difficult (super-cooled circuitry)

Increased Data Bus Width

- Larger instructions or more instructions can be executed at one time.
- Reduces the number of fetches to main memory by transferring more data in a single fetch
- More transistors required which are smaller
- Densely packed transistors increases power consumption and heat dissipation is an issue.

Increased Cache Memory

- Registers are fast but only hold one piece of information
- Register capacity is maximum instructions size (word)
- Cache improves performance with more instructions stored on the CPU (Level-1 Cache)

Reading Review 8

Having read page 29-30, answer the questions below.

1. Explain how cache memory helps to improve system performance.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

2. Explain how the following improves system performance:

a) Increasing data bus width

_____
_____
_____
_____
_____

b) Increasing clock speed

_____
_____
_____
_____
_____

Environmental Impact

Intelligent Systems

An intelligent system has the ability to act on behalf of a user. In the past human control was always necessary to use systems however smart heating and home systems now have the ability to allow users to establish settings by using an app or computer software.

The systems can use these settings and can often make decisions without further human interaction. They can make use of external factors to make decisions. These external factors include weather, time of day or temperature.

Heating systems

Smart heating systems use a variety of ways to control the amount of heat required in our homes. Using activity sensors, some smart systems learn the temperatures that you prefer in certain rooms and at what times. Monitoring the activity in rooms can mean that the smart system adjusts the heating up or down depending on whether there is unusual activity in the house. The thermostat is connected to Wi-Fi and can be manually controlled by using an app on your phone. This allows you to turn the heating system off if you are not going home or to turn it on so that it is at the optimum temperature if you are coming home early.

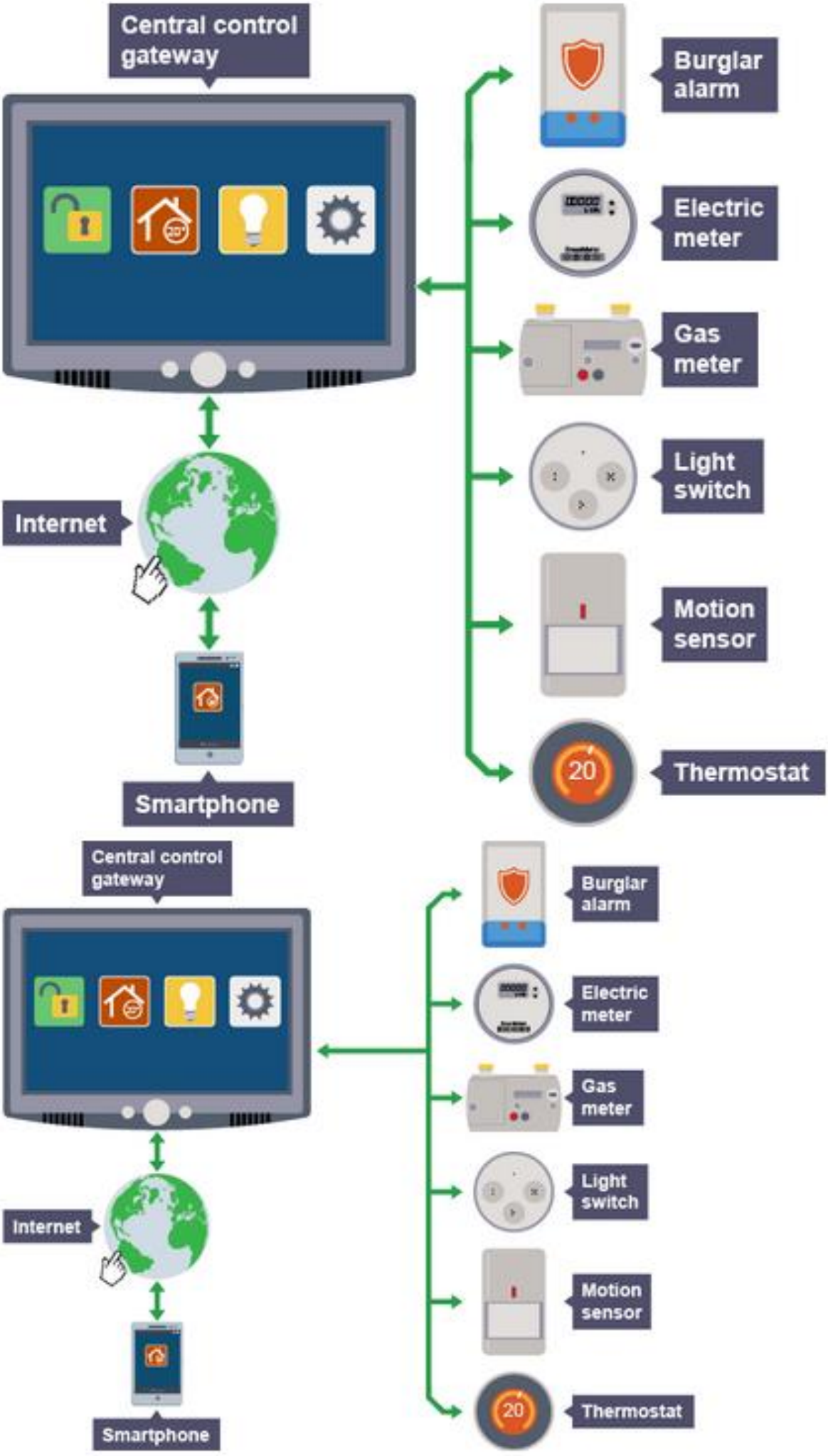
Traffic control

Vehicles are considered one of the main contributing sources of greenhouse gas. Studies in the European Union showed that transport causes 25% of all carbon dioxide emissions. Vehicles consume greater amounts of fuel when they are constantly accelerating and braking in traffic jams. The optimum speed for low fuel consumption and low emissions is between 45 and 65 miles per hour.

Intelligent transport systems use software and hardware, along with information and communications technologies, to improve the efficiency and safety of transport networks. They use a variety of information from cameras and sensors, along with control of traffic signals, to try to keep traffic moving, reducing the amount of harmful emissions. Cars with individual navigation systems use satellite information on traffic flow to guide drivers away from traffic congestion and on to more free-flowing routes.

Car management systems

A number of different car management systems are used to reduce the impact on the environment.
Start-stop systems automatically shut down the engine when the car is not moving — this reduces the amount of time the engine spends idling, reducing fuel consumption and emissions. The car automatically re-starts when the accelerator is pressed, which is most advantageous for vehicles that spend significant amounts of time waiting at traffic lights or frequently come to a stop in traffic jams.
Engine control units use sensors to ensure the engine's air/fuel ratio can be controlled very accurately, ensuring optimum fuel consumption and a reduction of carbon dioxide emissions.


Central control gateway
Burglar alarm
Electric meter
Gas meter
Light switch
Motion sensor
Thermostat
20
Internet
Smartphone
Central control gateway
Burglar alarm
Electric meter
Gas meter
Light switch
Motion sensor
Thermostat
20
Internet
Smartphone

Reading Review 9

Having read page 33-35, answer the questions below.

1. What is an intelligent system?

_____
_____
_____
_____

2. Explain how the following intelligent systems work and the benefits of each:

a) Heating Systems

_____
_____
_____
_____
_____

b) Traffic Control Systems

_____
_____
_____
_____
_____

c) Car Management Systems

_____
_____
_____
_____
_____

Security Risks & Precautions

Computer Misuse Act

The Computer Misuse Act was designed to protect individuals and businesses against computer attacks such as:

- Gaining **unauthorised access** to a computer to view data, modify data or commit a crime.
- **Hacking** into a computer network or accessing a computer networking without appropriate authorisation.
- Purposefully creating or distributing malicious software such as **viruses**.

The Computer Misuse Act is divided into **three main** offences:

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material.

1. Unauthorised access to computer material:

- Causing a computer to perform any function with intent to secure access to any program or data held in a computer or network
- Gaining any unauthorized access to a computer or a network or any particular program or data stored on the computer or network
- Accessing or using a computer or network by using another person's user name, e-mail, password etc. without appropriate authorisation.

2. Unauthorised access with intent to commit or facilitate commission of further offences:

- Interfering with the normal operation of the system with the intent to cause harm or damage. E.g. changing passwords and settings to prevent others accessing the system

- Purposefully spreading malicious and damaging software such as viruses

- Using hardware and software to access, copy, modify or steal data without appropriate authorisation. E.g. using phishing or keylogging to gain access to a computer system

3. Unauthorised modification of computer material:

- Unauthorised access to modify computers include altering software and data

- Deleting or making changes to a file with the intent to cause damage to an individual or company

- Purposely introducing viruses onto a computer or network

If found guilty of breaching the Computer Misuse Act the penalties include up to 10 years in prison and/or a fine.

Tracking Cookies

Cookies are text files that contain information about browsing habits, such as the website visited and the username used to access the site.

They can also track things like the amount of time spent on a site, or the multimedia that was watched as well as user defined browser settings.

Cookies can be helpful for those using the same system to access the internet on a regular basis. They can make browsing seem less demanding by remembering preferences and usernames. This saves time the next time you visit a website.

However, there are **'tracking cookies'** and these cookies are designed to send as much data as possible to external servers/third parties.

Sometimes the tracking cookie is used for market research and no theft of data is intended but on other occasions programmers can set the tracking cookie up to send them usernames and personal details.

As well as concern around identity theft, these cookies can be used to target users with personalised adverts.

Reading Review 10

Having read pages 38 – 40 answer the questions below.

1. Explain the three main offences of the computer misuse act.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

2. Explain how tracking cookies can be used for malicious purposes.

_____

_____

_____

_____

Denial of Service

Denial of Service(DoS) Attack

A DoS attack is a deliberate attempt to prevent legitimate users of a network from accessing the services provided by the server or connected systems.

The classic DoS attack will come from a single computer sending multiple requests to the server.

Denial of service attacks usually aim to overload servers or systems with requests for data or access to resources like the processor or main memory.

Some denial of service attacks also exploit weaknesses, either in the security system or network infrastructure.

Symptoms and effect of Denial of Service attacks

Common symptoms of a Denial of Service attack include:

- slow performance when trying to log in to a web based system, as the system may be under attack
- slow network performance in general
- inability to access a website as the web server may be under attack

The effect is inconvenience and **disruption for users** who are denied access to services they expect to use.

Cost of Denial of Service attacks

For organisations that fall victim to a Denial of Service attack the costs usually fall into two categories:

- loss of income
- repair costs to bring software and efficiency back to pre-attack level

A site selling goods online would be unable to receive orders, leading to a loss of income. Attackers often plan attacks when they know that an organisation would expect many users to want to access the server or services.

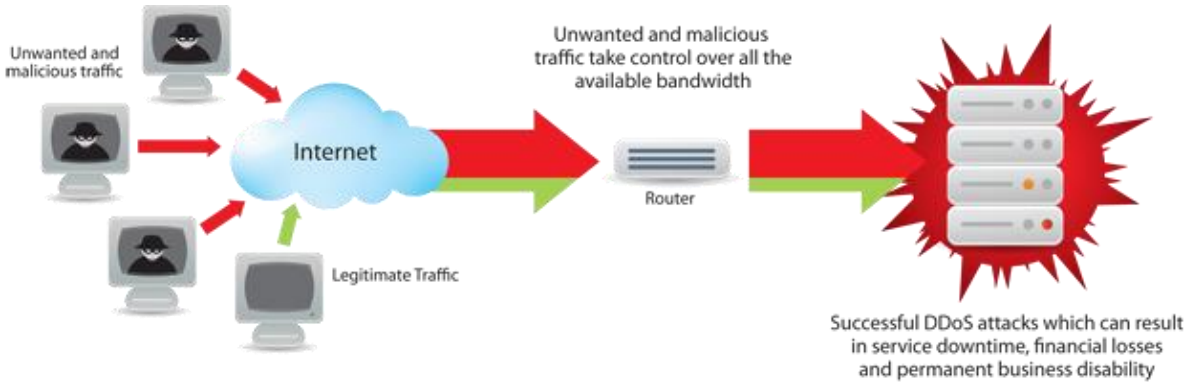
Organisations will often have to call in staff out with their normal working hours or hire additional staff to get the server back up and running again as soon as possible. While most attacks are resolved within 1 or 2 hours, the performance of the server may not be that of pre-attack performance for a number of hours.

Type of Denial of Service attacks

<u>Bandwidth consumption</u>

Bandwidth consumption is a fairly general term to describe overloading a server or individual system with too many data packets or requests at the same time, creating an overload in network traffic.

When this happens, the system is unable to send or receive data as the bandwidth available is used up by all of the network traffic/packets trying to get to the system.



Resource starvation

Resource starvation attacks are designed to use up system resources.

Processors and **main memory** are examples of resources that can be attacked, as is backing storage.

An example could be sending data over a network that requires the same process to repeat over and over again. By ensuring that the processor is always dealing with a recurring request, other processes cannot get enough processor time to execute properly.

Main memory and **backing storage** can also be targeted, an example of a method of starving available memory on a server could be to constantly add items to the basket of a server for an e-commerce site. This can be achieved by writing a script that adds millions of items.

Scripts can also be created and sent to a server requesting that thousands of new user accounts be created. Each new account would add to demands on backing storage and eventually starve available storage for legitimate requests.

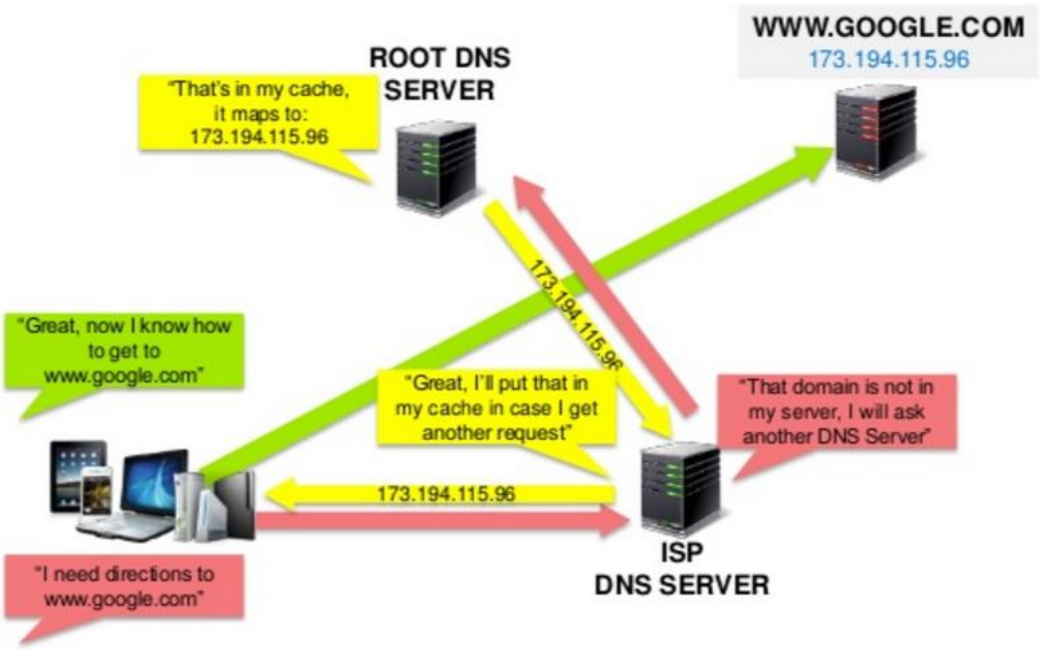
Domain Name Server attacks

We all know that we can type in a web address (URL) to access a web page. But computers must use IP addresses to communicate with each other.

This means that when you type in the web address, there has to be a way for your computer to find out the IP address for the web server which holds the web page.

Domain name servers (DNS) hold a directory of domain names and their associated IP addresses.

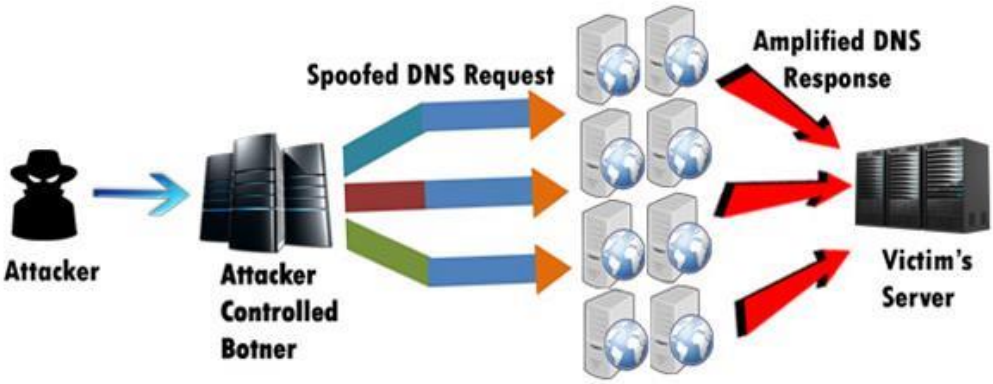
When a URL is entered into the browser, the default DNS server is contacted. The DNS looks up the web address in its directory and **replies** to the client computer with the corresponding IP address.



Domain Name Servers can be used in a Denial of Service attack when:

- attackers use 'spoofing' - using the IP address of a system that they want to attack without permission to use that IP address
- they send lots of queries to different Domain Name Servers at the same time
- the results of the queries are sent back to the IP address of the system they are targeting
- the attacked system is overloaded with replies from lots of different Domain Name Servers, all trying to send the website IP address that matches the domain name sent with the query

The sheer volume of replies that the targeted system receives will result in bandwidth consumption and overload the system so that it cannot send and receive data to and from the network.



Reasons for launching a Denial of Service attack

Reasons for launching Denial of Service attacks vary but broadly fall under one of three categories:

- Personal motive
- Political motive
- Financial gain

Some organisations are formed with the intention of creating distributed denial of service attacks. A portion of these groups do so for personal reasons, often linked to their ability to bring down large networks or organisations.

While many more are motivated by political and financial reasons there are those who engage in denial of service attacks as an area of personal interest.

There are also those who may have a personal grievance against an organisation or individual, who then choose to launch attacks if they have the necessary expertise.

Many more are motivated by politics or social issues. There are some well-known self-appointed civilian groups who work together online to target organisations who they perceive as incorrect or guilty of a political or social scandal.

National security groups have also been known to attack the networks of rival nations and there are likely to be many attacks every day that target the various military and defence agencies around the world.

Criminals also make use of distributed denial of service attacks, often in the hope that they can threaten organisations or users with an attack that can be prevented if they are willing to pay a fee. Some people are also willing to be hired by others if they have the technical knowledge necessary to carry out attacks on behalf of another person or group.

Reading Review 11

Having read pages 42 – 46 answer the questions below.

1. Explain the difference between a Denial of Service attack and a Distributed Denial of Service attack.

   _____
   _____
   _____
   _____
   _____

2. What are the symptoms of a Denial of Service attack?

   _____
   _____
   _____
   _____
   _____

3. What is the effect on users of a Denial of Service attack?

   _____
   _____
   _____
   _____

4. State four ways in which a Denial of Service attack can be conducted.

   _____
   _____
   _____
   _____

5. Give a brief description of each of the different types of Denial of Service attack.

1._____

_____

_____

_____

2._____

_____

_____

_____

3._____

_____

_____

_____

4._____

_____

_____

_____

_____

6. Describe three reasons why people carry out Denial of Service attacks.

_____

_____

_____

_____

_____

_____

_____

Security Precautions

Encryption

Encryption is the process of changing data so that it cannot be understood by a third party. **Decryption** is the reverse.

Data 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.

Encrypted data is known as **ciphertext**. Ciphertext cannot be read without first being decrypted.

There are two types of encryption:

- Conventional (Symmetric) Encryption
- Public Key (Asymmetric) Encryption

Symmetric Encryption

Conventional encryption is the simplest form of encryption. Also known as symmetric encryption as data is encrypted and decrypted using **the same key**.

Data (plain text) is encrypted using a secret key and encryption algorithm. Both parties must have a copy of the secret key which must also be kept secure.

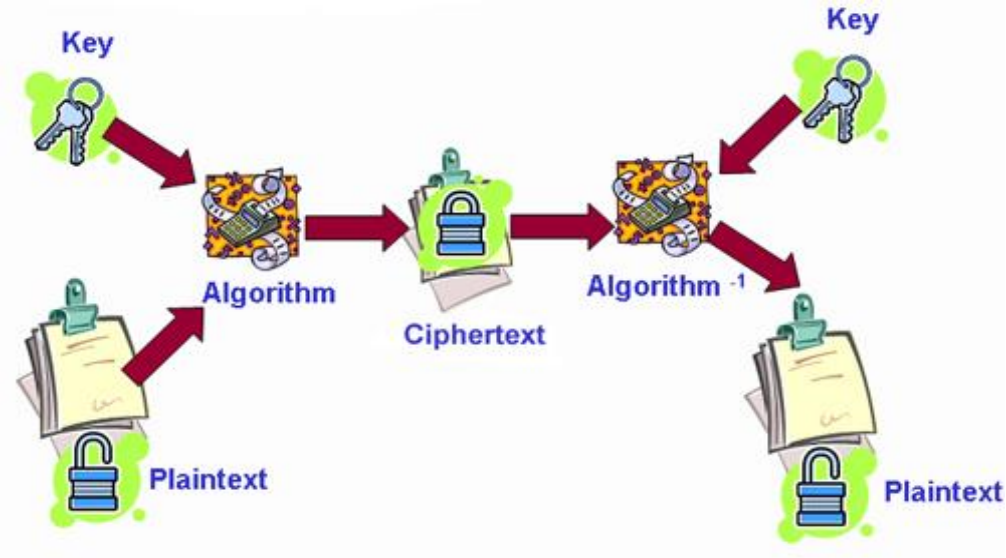
Encryption Key

A **key** is a long sequence of bits used by encryption / decryption algorithms.

To crack some ciphertext encrypted with a 64-bit key by trying every combination of keys possible means you have 2^64 possible combinations (18 followed by 18 naughts).

If you have a computer that can carry out one encryption operation every millisecond, it will take about 292 million years to find the correct value.

Plain text is combined with the secret key and encryption algorithm to produce ciphertext.



Ciphertext is then combined with the secret key and the decryption algorithm to produce plain text.

Problems with Symmetric Encryption

- The secret key must initially be shared between both parties.
- So unless a secure method exists (physically meeting each other) then the system is inherently insecure.
- If an attacker obtains a large number of encoded messages, letter or word frequency tables could be used.

Despite these problems, symmetric encryption is reliable and allows for fast decryption. It is still a very popular method of encryption and is used by many large organisations to manage the transmission of online communication.

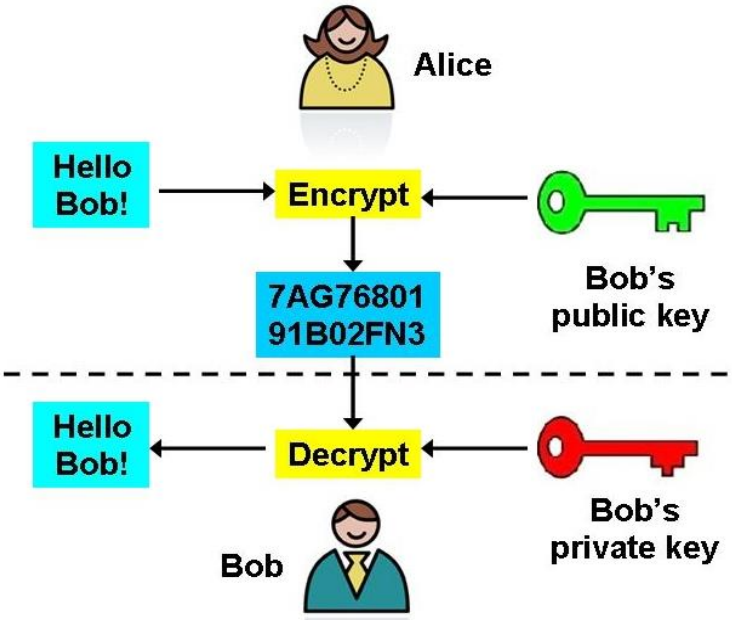
Public Key Encryption

Public Key Encryption is more complicated and slower but more secure. Also known as **asymmetric encryption** as data is encrypted and decrypted using the **different keys**.

Public key can be made available to anyone but only the **owner** of the public key can decrypt it using a **private key**.

Since a different key is used for decryption, it always remains secret and is therefore more secure.

Plain text is combined with the **recipients public key** and **encryption** algorithm to produce ciphertext.



Ciphertext is combined with the **recipients private key** and **decryption** algorithm to produce plain text.

"Key" points

Encrypting – message is encrypted using the recipients public key

Decrypting – message can only be decrypted using the recipients private key

Reading Review 12

Having read pages 49 – 51 answer the questions below.

1. Describe how Conventional Encryption works.

_____

_____

_____

_____

_____

2. What is the main problem with Conventional Encryption?

_____

_____

_____

_____

3. Explain how Public Key encryption improves security of transmitted data.

_____

_____

_____

_____

_____

_____

4. Sally uses Public Key encryption to send a message to Ben. Referring to keys involved, describe how this message would be encrypted and decrypted.

_____

_____

_____

_____

Digital Signature

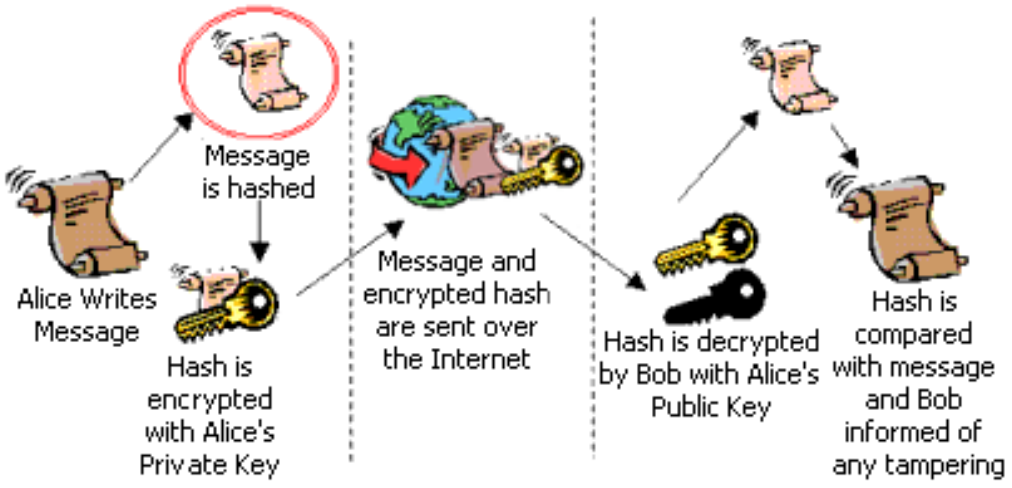
A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document has not been tampered with.

Sending Computer

- Sender must first **purchase encryption software** allowing him to create public and private key
- Hashing algorithm is applied to the data to be transmitted creating a unique **message hash** (mathematical summary).
- Message hash is encrypted using the **<u>sender's</u> private key**.

Receiving Computer

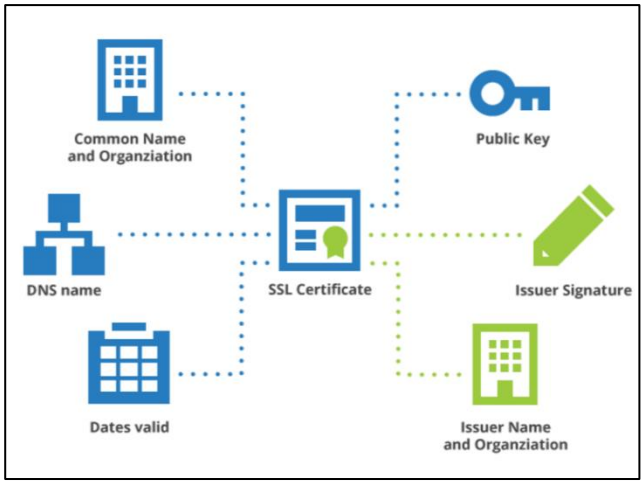
- **<u>Sender's</u> Public key** is used to decrypt the message hash – if this works then it proves the sender's identity.
- Hashing formula is then applied to the data to calculate its own message hash and this is compared to the one transmitted.
- If they match then the data has arrived untampered.



Digital Certificate

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**.



A digital certificate 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

- A serial number that is used to uniquely identify the certificate, the individual or the entity identified by the certificate
- The algorithm that is used to create the signature
- The Certification Authority that verifies the information in the certificate
- The date that the certificate is valid from and the date that the certificate expires
- The public key and the thumbprint algorithm (to make sure that the certificate itself is not modified)

A digital certificate gives the user of a site confidence that:

- The site is authenticated e.g. certificate issued by (certification) authority
- The site is regulated

Reading Review 13

Having read pages 53 – 54 answer the questions below.

1. What is a digital signature?

_____

_____

_____

2. Describe how a digital signature is used to authenticate messages

_____

_____

_____

_____

_____

_____

_____

3. What is a digital certificate?

_____

_____

_____

_____

4. Why are digital certificates used?

_____

_____

_____

5. What information is contained in a digital certificate?

_____

_____

_____