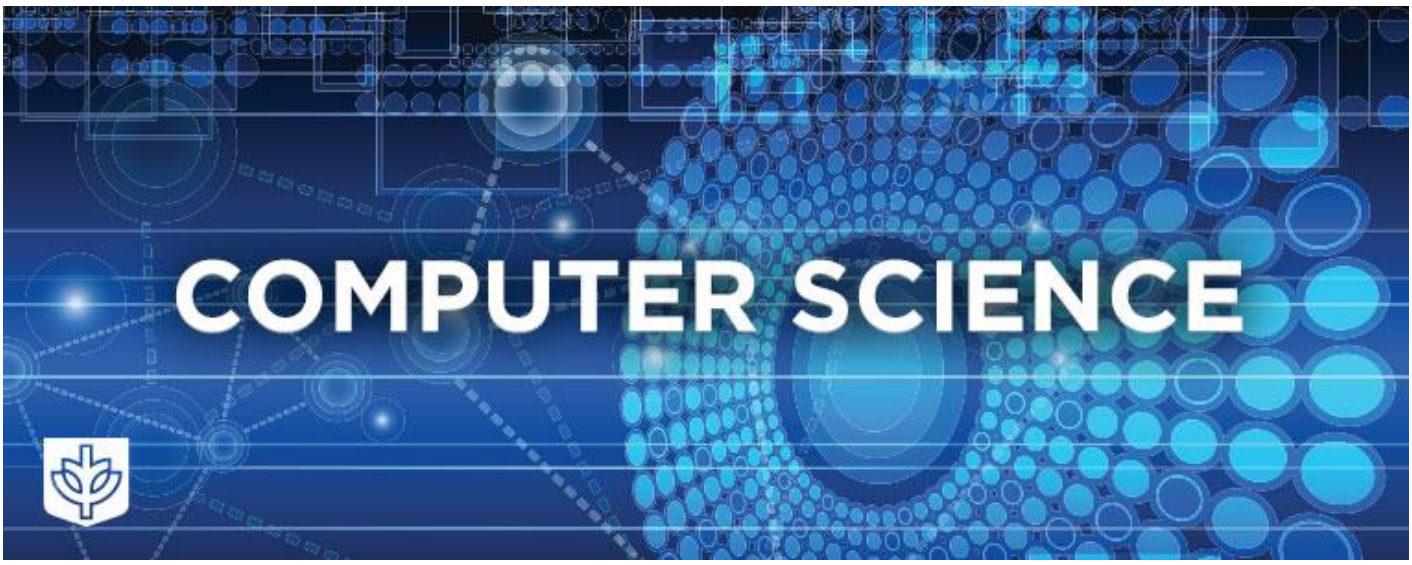
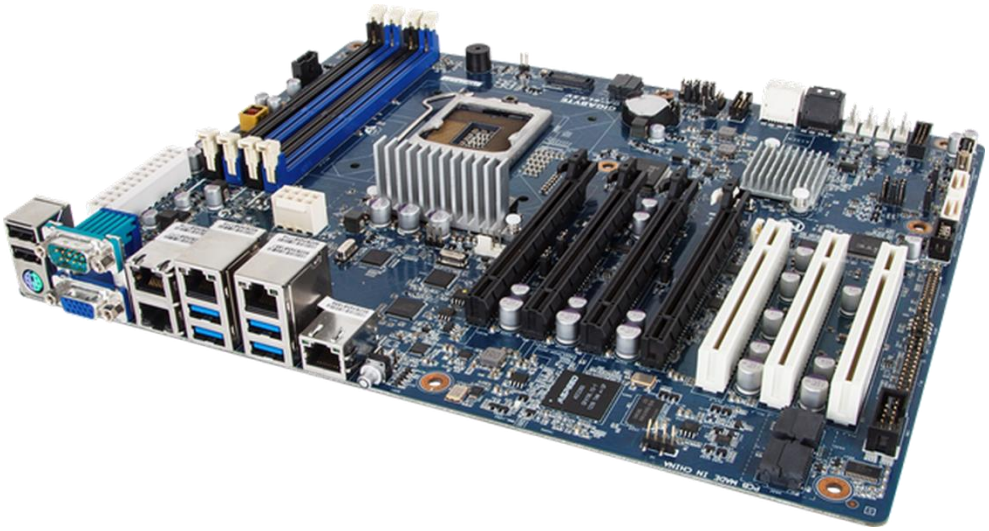


HIGHER

COMPUTING SCIENCE

COMPUTER SYSTEMS



DATA REPRESENTATION

NATIONAL 5 REVISION

Convert Binary to Denary

Positive integers are stored in the computer using their place values and can be used to convert Binary to Denary.

Place value	64	32	16	8	4	2	1
Binary value				1	0	0	1

8 + 0 + 0 + 1 = 9

Convert Denary to Binary

To convert a denary integer into its binary equivalent you follow these instructions. We will use the example of 85.

1. *Draw out your place values table for binary.*

128	64	32	16	8	4	2	1

2. *Work out which is the smallest number that will divide into your denary number once and put a 1 under its place value in this case 64 is the largest that will divide into 85 once so a zero is put under the 128 and a 1 under 64.*

128	64	32	16	8	4	2	1
0	1						

2. *We have now used 64 of our 85 leaving us 21 (85-64 = 21). We simply repeat step 2. until we have nothing left. 16 is the largest that will divide into 21 so a 0 goes under the 32 and 1 under 16.*

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

3. *We have now used 16 of our 21 leaving us 5 (21-16 = 5). 8 will not divide into 5 once therefore we put a 0 under the 8. 4 will divide into 5 once so we put a 1 under the 4. We have now used 4 of our 5 leaving us 1 (5-4 = 1). 2 will not divide into 1 once therefore we put a 0 under the 2. 1 will divide into 1 once so we put a 1 under the 1.*

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

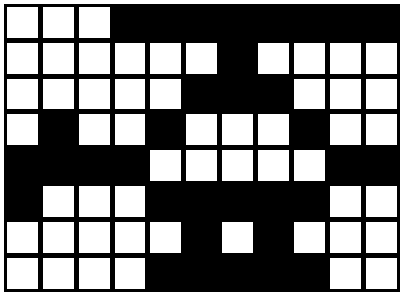
Real Numbers

A real number is a number that can have a decimal/fractional part to it. Real numbers are represented using floating point representation. Floating point representation stores the number in the mantissa and exponent.

Characters

Characters are stored using the extended ASCII code. Each character is given a unique number and stored using 8 bits of memory e.g. A = 01000001 in binary.

Bitmapped Graphics



0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	0	1	1	1	0	0	0
0	1	0	0	1	0	0	0	1	0	0
1	1	1	1	0	0	0	0	0	1	1
1	0	0	0	1	1	1	1	1	0	0
0	0	0	0	0	1	0	1	0	0	0
0	0	0	0	1	1	1	1	1	0	0

A bit-mapped graphic is stored as a 2-dimensional array of pixels where each pixel stores the colour of that pixel.

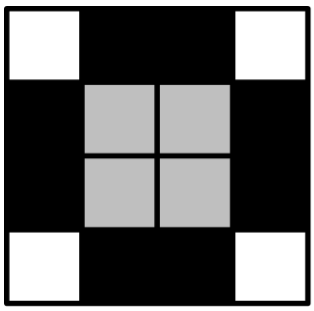
Each pixel in a black and white bit-mapped graphic is stored using 1-bit of memory. By counting the pixels, you can work out how much memory it takes to store the picture. The above graphic takes 88 bits of memory.

Colour graphics require more than 1-bit of memory to store a pixel.

- *8-bit graphics require 8 bits of memory to store the colour of each pixel.*
- *24-bit graphics require 24 bits of memory to store the colour of each pixel.*

This significantly increases the amount of memory required to store a graphic.

The example opposite uses 2-bit colour i.e. it takes 2-bits per pixel to store the colour of the pixel.

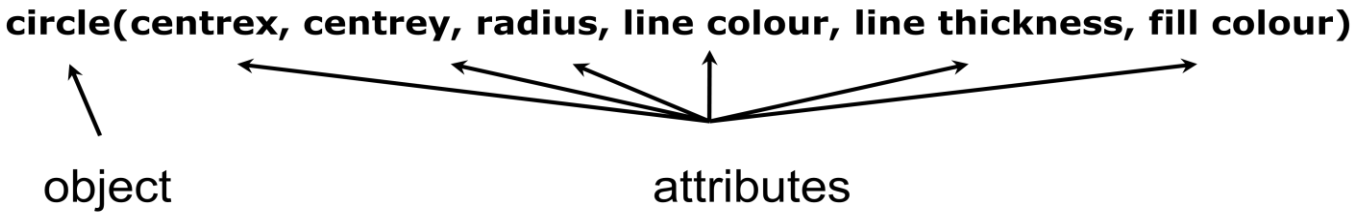


00	01	01	00
01	10	10	01
01	10	10	01
00	01	01	00

00 = white 01 = black 10 = grey

Vector Graphics

Vector graphics store a picture by storing each object's attributes. A circle might be stored as:



i.e. it doesn't store the picture itself but the instructions of how to draw the picture.

A line might be stored as

line(startx, starty, end x, endy, line colour, fill colour).

When stored in the computer each attribute would be stored as a binary number.

POSITIVE AND NEGATIVE INTEGERS

At National 5 we only used positive integers. Most numbering systems have both positive and negative numbers therefore we need a method of representing these. This is known as **Two's Complement**.

In Two's complement, the most significant bit (the leftmost bit) indicates whether the number is positive or negative. If the most significant bit is a 1 then it is a negative number, if it is a 0 then it is positive.

If we were using 8-bits then using two's complement we would know Example 1 is a positive number (because the leftmost bit is a 0) and Example 2 is a negative number (because the leftmost bit is a 1).

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

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

Converting a negative denary number into its twos complement binary number

To convert a negative denary number into its two complement representation you:

- work out the positive binary number
- invert all the bits (so a 1 becomes a 0 and a 0 becomes a 1)
- then add 1.

To show how -5 would be represented as an 8-bit binary number:

	128	64	32	16	8	4	2	1
Calculate binary of +5	0	0	0	0	0	1	0	1
Invert all the bits	1	1	1	1	1	0	1	0
Add on 1	1	1	1	1	1	0	1	1

Therefore the two's complement representation of -5 would be 11111011.

Here are three negative integers. Show how each would be represented using 8-bit two's complement:

a) Show how -26 would be stored as an 8-bit two's complement binary number.

	128	64	32	16	8	4	2	1
Calculate binary of +26								
Invert all the bits								
Add on 1								

b) Show how -77 would be stored as an 8-bit two's complement binary number.

	128	64	32	16	8	4	2	1
Calculate binary of +77								
Invert all the bits								
Add on 1								

c) Show how -40 would be stored as an 8-bit two's complement binary number.

	128	64	32	16	8	4	2	1
Calculate binary of +40								
Invert all the bits								
Add on 1								

Converting a two's complement binary number to denary

Before doing anything, we need to decide if the two's complement is a positive or negative number.

Positive two's complement number

Firstly you need to look at the most significant bit (the leftmost bit); if it is a 0 then it is positive and simply convert the number to decimal. For example:

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

Because the leftmost bit is a 0 then we know the number is positive so we simply add 32 + 4 + 1 = +37.

Negative two's complement number

If the most significant bit (the leftmost bit); is a 1 then we have to convert the number to a positive number then work out the denary equivalent. The good news is that you do this in exactly the same way you converted a positive number to negative i.e.

- invert all the bits (so a 1 becomes a 0 and a 0 becomes a 1)
- then add 1
- convert to denary.

For example: Convert the two's complement binary number 11111011 to denary.

Because the most significant bit is a 1 we know it is a negative number therefore we need to convert it to a positive number first.

	128	64	32	16	8	4	2	1
	1	1	1	1	1	0	1	1
Invert all the bits	0	0	0	0	0	1	0	0
Add on 1	0	0	0	0	0	1	0	1

We can now convert this to denary by 4 + 1 = -5 (Don't forget to put the negative sign in front of it).

Therefore the denary equivalent of two's complement 11111011 is -5.

a) Convert the two's complement binary number 11101001 into denary.

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

Invert all the bits

Add on 1

Denary equivalent _____

b) Convert the two's complement binary number 00010100 into denary. Be careful!!

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

Invert all the bits

Add on 1

Denary equivalent _____

c) Convert the two's complement binary number 11010000 into denary.

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

Invert all the bits

Add on 1

Denary equivalent _____

Calculating the range of positive and negative integers that can be stored

Where you have a fixed number of bits to represent a two's complement number, you can calculate the range of numbers that can be stored i.e the lowest negative number to the highest positive number.

For example: if we had two bits then we could store 4 numbers from -2 to +1.

Denary	2-bit Two's complement
-2	10
-1	11
0	00
1	01

The formula to calculate the range is:

$-(2^{(bits-1)})$ to $2^{(bits-1)} - 1$

e.g. If 8 bits was used to store a number then the range would be :

$-(2^{(8-1)})$ to $2^{(8-1)} - 1 = -128$ to $+127$

If you find this formula too difficult to remember then you can use an easier way:

1. Calculate the total number of numbers that can be stored by using 2^{bits}.
2. Half the number and this is the negative value
3. Reduce this number by 1 and this is the positive value

For example: What range of positive and negative numbers can be used using 16 bits?

1. $2^{16} = 65536$
2. $65536 / 2 = 32768$ this is the negative value
3. $32768 - 1 = 32767$ this is the positive value
4. Therefore the range of numbers that can be stored is -32768 to +32767.

Here are 3 for you to try:

a) Calculate the range of two's complement numbers that can stored using 24 bits.

_____

b) Calculate the range of two's complement numbers that can stored using 7 bits.

_____

c) Calculate the range of two's complement numbers that can stored using 18 bits.

_____

FLOATING POINT REPRESENTATION

A real number is a number that can have a decimal/fractional part to it. To represent a real number in binary we use *floating point representation*. Floating point representation stores the number in the *mantissa* and *exponent*.

The structure of a floating point number is: mantissa x base^{exponent}

For example: in decimal 217.46 could be represented as 0.21746×10^3

where 21746 is the mantissa, 10 is the base and 3 is the exponent.

To work out the mantissa and exponent you need to :

- move the point all the way so the number is a fractional value
- the entire number without the point is the mantissa
- the number of places the point was moved (expressed as a two's complement binary number) is the exponent.

Example 1 - How would 1101.0011 be represented in binary floating point representation using 16 bits for the mantissa (including the sign bit) and 8 bits for the exponent?

Fixed Point	Floating point	Sign (1 bit)	Mantissa (15 bit)	Exponent (8 bit)
1101.00111	$0.110100111 \times 2^{100}$	0	110100111000000	00000100

Note the exponent is 00000100 as the binary point was moved +4 places to the left and the 8 bit two's complement binary of +4 = 00000100

Here are two for you to do:

a) Show how 10100.1111 would be represented in binary.

Fixed Point	Floating point	Sign (1 bit)	Mantissa (15 bit)	Exponent (8 bit)
10100.1111				

b) Show how 11.1101 would be represented in binary.

Fixed Point	Floating point	Sign (1 bit)	Mantissa (15 bit)	Exponent (8 bit)
11.1101				

Sometimes we have to move the binary point to the right rather than the left this gives a negative exponent.

Example 2 - How would 0.0001001 be represented in binary floating point representation using 16 bits for the mantissa (including the sign bit) and 8 bits for the exponent?

Fixed Point	Floating point	Sign (1 bit)	Mantissa (15 bit)	Exponent (8 bit)
0.0001001	1001×2^{-11}	0	100100000000000	11111101

Note the exponent is 11111101 as the binary point was moved 3 places to the right (i.e -3 places) and the 8 bit two's complement binary of -3 = 11111101

Here are two for you to do:

a) Show how 0.0010011 would be represented in binary floating point representation using 16 bits for the mantissa (including the sign bit) and 8 bits for the exponent.

Fixed Point	Floating point	Sign (1 bit)	Mantissa (15 bit)	Exponent (8 bit)
0.0010011				

b) Show how 0.00000101 would be represented in binary floating point representation using 16 bits for the mantissa (including the sign bit) and 8 bits for the exponent.

Fixed Point	Floating point	Sign (1 bit)	Mantissa (15 bit)	Exponent (8 bit)
0.00000101				

Lastly, sometimes the mantissa is a negative value. For example:

Example 3 - How would -101.00011 be represented in binary floating point representation using 16 bits for the mantissa (including the sign bit) and 8 bits for the exponent?

Fixed Point	Floating point	Sign (1 bit)	Mantissa (15 bit)	Exponent (8 bit)
-101.00011	-10100011×2^{11}	1	101000110000000	00000011

Here are two for you to do:

a) Show how 0.0010011 would be represented in binary floating point representation using 16 bits for the mantissa (including the sign bit) and 8 bits for the exponent.

Fixed Point	Floating point	Sign (1 bit)	Mantissa (15 bit)	Exponent (8 bit)
-1.10111				

b) Show how 0.00000101 would be represented in binary floating point representation using 16 bits for the mantissa (including the sign bit) and 8 bits for the exponent.

Fixed Point	Floating point	Sign (1 bit)	Mantissa (15 bit)	Exponent (8 bit)
-0.00011				

Range and Precision of Floating Point Numbers

The number of bits allocated to a floating point number is usually fixed. For example: if you had a fixed 40 bits for storing a floating point number then 32 bits could be allocated to the mantissa leaving 8 bits for the exponent.

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 that can be stored.

Here is a simple example:

Pi can be expressed as 3.14 or as 3.14159265359

Obviously, the second value is more precise than the first value because more bits have been allocated to the mantissa.

This leads to some rules:

- Increasing the number of bits allocated to the mantissa increases the precision of the number. Conversely, decreasing the number of bits allocated to the mantissa decreases the precision of the number.

- Increasing the number of bits allocated to the exponent increases the range of numbers that can be stored. Conversely, decreasing the number of bits allocated to the exponent decreases the range of numbers that can be stored.

Because there is a fixed number of bits for a floating point number, increasing either the number of bits allocated to the mantissa or exponent will reduce the number of bits to the other. Therefore:

- Increasing the number of bits to the mantissa increases the precision but decreases the range as fewer bits are available for the exponent.

- Increasing the number of bits to the exponent increases the range but decreases the precision as fewer bits are available for the mantissa.

CHARACTERS

Extended ASCII is an 8-bit method of storing characters such as:

- all the English numbers, letters (upper and lower) and punctuation marks in the alphabet
- foreign language symbols e.g. é, ö, ê
- control characters e.g. tab, line feed, carriage return

However, being an 8-bit code, it is restricted to 2^8 i.e. 256 characters which may be enough for the characters listed above but was not enough to store the characters of a large number of foreign languages. Therefore a new system was introduced called Unicode.

Unicode

Originally, Unicode was a 16-bit code therefore allowed 2^{16} i.e. 65536 characters to be identified.

Advantages of Unicode over extended ASCII	• Because a much larger number of characters could be identified additional language characters could be identified e.g. Cyrillic, Latin etc. • The first 128 codes were identical to the original ASCII codes so compatibility with ASCII was maintained.
Disadvantage of Unicode over extended ASCII	• Because it was a 16-bit code, each character took double the amount of memory to store as ASCII so file sizes increased as did transmission times.

A further version of Unicode was developed which was a 32-bit code. This allowed 2^{32} characters to be identified. This allowed for nearly all languages including Chinese and Japanese to be stored.

ADVANTAGES AND DISADVANTAGES OF BITMAPPED GRAPHICS

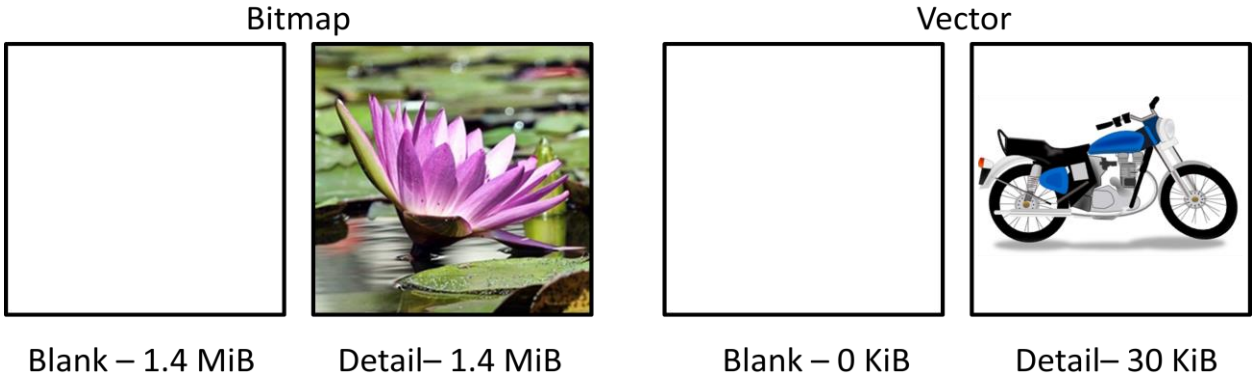
As you will recall from National 5 there are two means of representing graphics Bitmapped and Vector Graphics. Both have their particular uses as well as advantages and disadvantages.

File Size

A bitmap graphic nearly always has a much larger file size than a vector graphic.

A bitmapped graphic stores every pixel therefore even a blank graphic where every pixel is white will have a very large file size. When we change any pixel's colour (or add additional detail to the image) it has no effect on the file size as it is already storing every pixel.

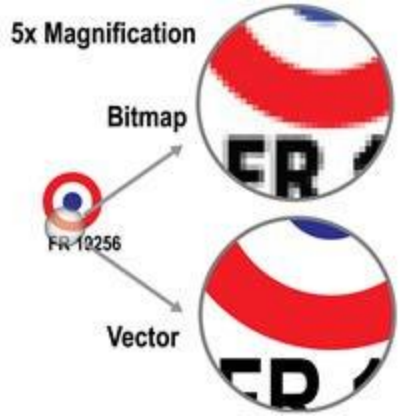
A vector graphic however, only stores the instructions of how to draw each object and therefore takes a lot less storage than the equivalent bitmap. However, when you add extra objects to a vector graphic it does increase the file size (as it is storing more instructions how to draw the image). In theory, (although not in practice) a blank vector graphic would have no file size, whereas every object added to the graphic would increase the file size.



Scaling larger

Bitmap graphics are resolution dependent. This means that when you scale a bitmap graphic larger it will pixelate as you will be able to see the individual pixels making up the graphic.

Vector graphics are resolution independent and therefore when scaled larger will not pixelate.



Layering

Bitmap graphics are a 2-D array of pixels therefore you cannot put one pixel on top of another (i.e. you cannot layer pixels).

Vector graphics allow you to move objects behind or in front of other objects therefore they can be layered.

Uses

With bitmap graphics you can edit individual pixels therefore giving photo realistic pictures. They are therefore frequently used for photo editing purposes.

Vector graphics can only be made up of mathematically defined shaped like rectangles, ellipses, lines etc and therefore cannot create photo realistic pictures. They are therefore used for purposes like CAD (Computer Aided Drawing).

Summary of Advantages and Disadvantages of Bitmapped and Vector graphics

Criteria	Bit Mapped Graphics	Vector Graphics
Advantages	Can edit down to the individual pixel level. Adding extra detail to the picture does not increase the file size. Can create photo realistic images.	Have a small file size as only each objects' attributes are saved. Objects can be scaled larger without pixelating as they are resolution independent. Objects can be layered.
Disadvantages	Have a very large file size as every pixel needs to be stored. When scaled larger, pictures pixelate as they are resolution dependent.	Difficult to create photo-realistic images as can only work with objects. Adding extra objects to the picture increases the file size.

COMPUTER STRUCTURE

NATIONAL 5 REVISION

Processor

The processor (sometimes known as the central processing unit -CPU) is the part of a computer system that carries out the instructions of a computer program, to perform the basic arithmetical, logical, and input/output operations of the system.

*The processor is divided into three parts : **the control unit**, the **Arithmetic and Logic Unit (ALU)** and **registers**.*

Memory

Memory is a set of chips which store programs and data in the computer.

Buses

A bus is a group of wires used collectively to transmit information.

There are 2 buses that connect the processor and memory.

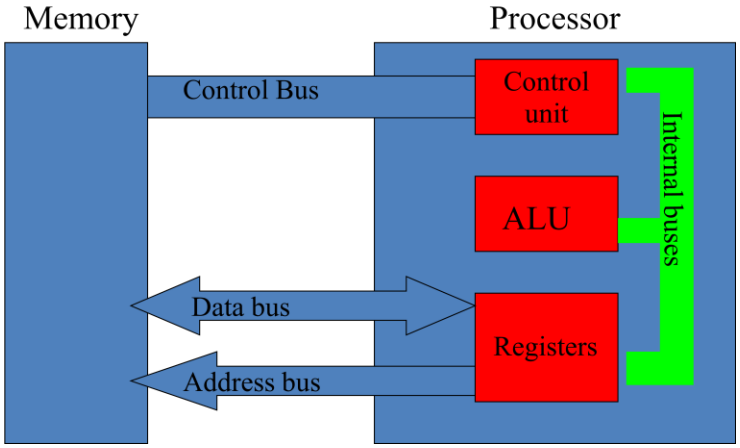
- *The **Address Bus** identifies the memory location that is going to be accessed. It is only a one-way bus as only the processor can identify the memory address.*
- *The **Data Bus** transfers data between the processor and memory and vice versa. It is a two-way bus as information can be written from the processor to memory and read from memory to the processor.*

STRUCTURE OF A COMPUTER

PROCESSOR

The processor can be considered to be made up of three components:

- Arithmetic and Logic Unit (ALU)
- Control Unit
- Registers



The **ALU** is where arithmetic operations (+-/*) and logical comparisons (AND OR NOT) are carried out.

The **Control Unit** sequences the fetching, decoding and execution of instructions. It does this by sending control signals to other parts of the computer.

Registers are temporary storage locations inside the processor itself. A register can be used for:

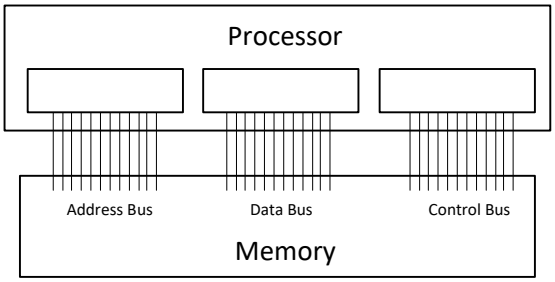
- holding the data/instruction being fetched/written (MDR)
- holding the current instruction being decoded and executed (IR)
- holding the memory address being accessed (MAR)

The main advantage of storing data in registers is because it is held in the processor itself, the data can be accessed much faster than reading it from main memory.

Older computers might only have a few registers whereas modern processors will have many more registers, with some having over 100 general purpose registers. The reason for this is that it is much more efficient (faster) to keep data in the processor rather than having to read and write the data to main memory.

BUSES

A bus is a group of wires used collectively to transmit information. There are three buses:



- Address bus
- Data bus
- Control bus

Address bus

The address bus is used by the processor to identify the memory location to be accessed.

It is a one-way bus as only the processor can identify the memory location to be accessed.

Data bus

The data bus is used to transfer data between processor and memory and vice versa.

It is a two-way bus as data can both be written from the processor to memory, and read from memory to the processor. Its size will usually be the same as the memory word size i.e. the number of bits the computer can process in a single operation.

Control bus

The control bus is used to identify and initiate the instruction to be carried out.

It is not really a bus at all as each line on the bus is used discretely. Some of the common lines in the control bus are:

- Read
- Write
- Clock
- Interrupt
- Reset

FETCH-EXECUTE CYCLE

A program may contain thousands of instructions but the processor can only execute one instruction at a time. The first instruction is fetched from memory into the processor where it is decoded and executed. Then the second instruction is fetched, decoded and executed, and so on until the program ends. This is known as the FETCH – EXECUTE CYCLE.

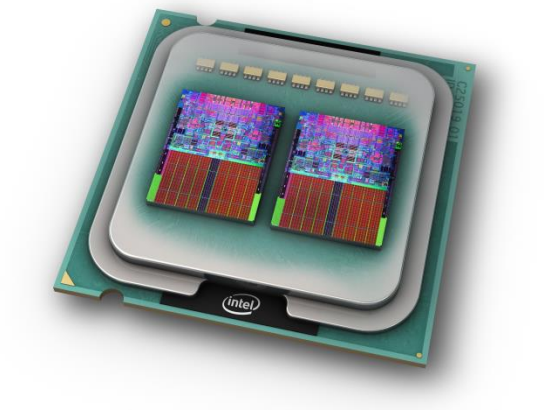
Steps in the fetch-execute cycle

	Steps	Effect
1.	Processor sets up address bus with the required address	This identifies the memory location to be read from.
2.	Processor activates the Read line on the control bus	This tells the processor that it is to read an instruction from the identified memory location to the processor.
3.	An instruction is fetched from the identified memory via the data bus and stored in the Instruction Register.	An instruction is transferred to the Instruction Register in the processor from the identified memory location via the data bus.
4.	The instruction in the instruction register is decoded and executed.	The instruction is decoded and executed. This may involve several more fetches of data from memory.

FACTORS AFFECTING SYSTEM PERFORMANCE

There are four factors that affect system performance:

1. Number of processors (cores)
2. Width of the data bus
3. Cache memory
4. Clock speed



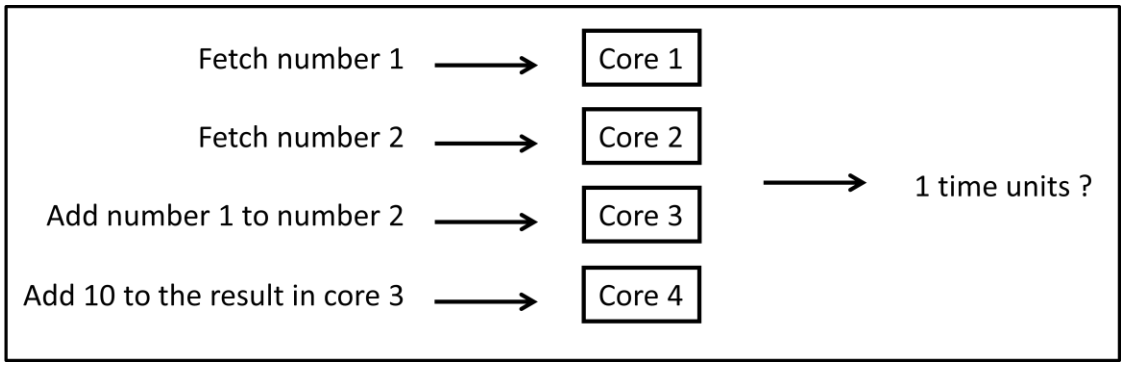
1. *Number of processors (Cores)*

You will probably have heard of dual core or quad core processors. These are where there is more than one CPU (central processing unit) in the one chip. A dual core processor has two CPU's in the one chip whereas a quad core processor has four CPU's in the one chip.

In theory, the more cores a processor has, the more instructions the processor can execute at the same time, thereby improving system performance.

However, the additional cores means additional heat generation so cooling of the processor is important and additional circuitry is required to coordinate the processing between the cores.

Is a quad core processor 4 times as fast as a single core processor? No. Take the following simple example:



You may think that a quad core processor could do all 4 processes at the same time. However, Core 3 must wait for cores 1 and 2 to fetch the numbers before it can add them together and core 4 must wait for Core 3 to finish the addition before it can carry out its instruction. So using a quad core processor would be faster than a single core but a 4-fold increase in speed would not happen.

Is a dual core processor where each core runs at 1.5Ghz faster than a 3GHz single core processor? No. For the same reasons as before one of the cores may have to wait for the other core to complete an instruction and this would reduce system efficiency.

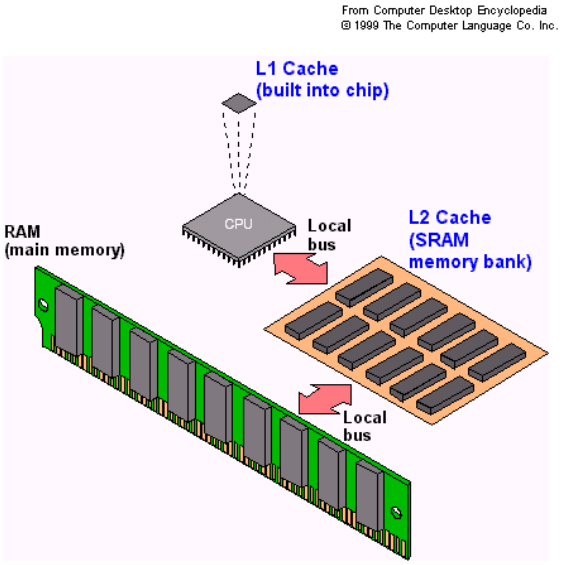
2. *Width of the data bus*

The width of a data bus is the number of wires in the data bus, each of which can transfer 1-bit of data at a time. So an 8-bit data bus could transfer 8 bits in a single fetch whereas a 64-bit data bus could transfer 64 bits. Therefore, increasing the width of the data bus should increase system efficiency.

If you think of this in terms of transferring ASCII characters a 64-bit data bus could transfer 8 ASCII characters in the same time it would take an 8-bit data bus to transfer 1 ASCII character.

3. *Cache Memory (pronounced 'cash')*

Reading and writing to RAM is fast, however, by using cache memory we can speed this process even further.



Cache memory is very high speed SRAM memory which is either on the processor itself or very close to it.

Your main memory (RAM) uses DRAM, whereas cache memory uses SRAM. SRAM has a much faster access time than DRAM so information read/written quicker.

Level 1 (L1) Cache is built into the CPU itself and is the fastest to access. Level 2 (L2) cache is closely adjacent to the CPU and is the next fastest to access. Main memory (RAM) is slower to access than either of the cache memories.

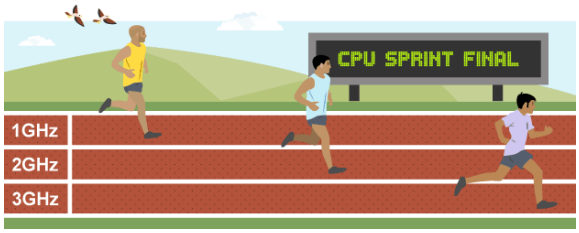
How does cache memory improve system performance?

1. Commonly used instructions can be moved into cache memory from RAM and therefore will be accessed faster. For example, if the processor was carrying out a loop 1000 times, each instruction within the loop would need to be fetched from slower access RAM 1000 times. However, when it is realised that these instructions are being used commonly they can be moved into cache memory so they can be accessed quicker, improving system performance.

2. When the processor is fetching data/instructions it first checks the L1 cache to see if it is there; if it is then a cache 'hit' is recorded and the data fetched from this faster SRAM memory. If the data is not in L1 cache then a cache 'miss' is recorded and the L2 cache is checked in the same way. Only if the data is not in any of the layers of cache memory does the processor fetch the data from slow access DRAM memory.

3. Cache memory uses high speed access SRAM memory.

4. *Clock Speed*



The clock is the electronic unit that synchronises all the activities of the processor by generating pulses at a constant rate. The clock speed is the frequency at which the clock generates these pulses and is used as an indicator of the processor's speed.

An instruction in the CPU can only start on a pulse of the clock, so the higher the clock speed the more instructions can be carried out per second so improving system performance.

Nowadays, clock speeds are measured in Gigahertz (GHz) with a typical processor speed being 3GHz. This means the CPU performs 3 billion cycles a second and if each instruction only took 1 cycle (unrealistic) then the CPU could carry out 3 billion instructions per second.

It may seem simple that to speed up a computer just increase the clock speed, but the faster the clock speed the more heat that is generated and this can overheat and damage the processor.

Does a 2 GHz Pentium Processor run at the same speed as a 2GHz AMD processor? No. There are two reasons why clock speed cannot be used accurately to compare processor speeds:

1. Different manufacturers measure clock speeds in different ways.

2. The architecture of the system, for example the data bus width will also affect the system performance.

Summary of factors affecting computer system performance

Number of processors (cores)	Increasing the number of cores in a chip to dual core, quad core or octa core, will improve system performance as several instructions can be carried out simultaneously. However, a quad core will not run four times as fast as a single core as some cores may need to wait for the results from other cores.
Width of the data bus	The width of the data bus determines how many bits can be transferred from processor to memory in a single fetch. Increasing the data bus width means that more bits can be transferred at the same time so will improve system performance.
Cache memory	Cache memory is a small amount of very fast SRAM either on the processor (L1 cache) or very close to the processor (L2 cache). Cache memory speeds up system performance by: 1. Using fast access SRAM rather than the slower access DRAM of main memory. 2. Moving commonly used instructions, for example a loop, into SRAM from DRAM speeding up access time. 3. When fetching data, checking if it is available from faster access cache memory before fetching it from main memory.
Clock Speed	The clock is the hardware that synchronises all activities of the processor. Instructions can only start on a pulse of the clock so increasing the clock speed means that more instructions can be started per second and hence system performance improved. Clock speeds are measured in gigahertz (GHz). Clock speed should not be used as the only comparator between different processors as different manufacturers use different methods of measuring clock speed and other factors affect system performance like the computer architecture.

ENVIRONMENTAL IMPACT

NATIONAL 5 REVISION

Making and using computers can have a significant impact on the environment. Some of the ways we can reduce this impact is by:

- *Set the computer to stand-by mode if there is 15 minutes of inactivity. This will power down the hard discs and turn off the monitors. Both will reduce the amount of energy being used.*
- *Choose monitor settings carefully; a very bright monitor uses more power than one that is slightly dimmer; set the monitor to stand-by mode after 15 minutes of inactivity.*
- *Set Power down settings; a large number of computers are left on all night when no-one is using them, for example the ones in your school. Setting the computers to automatically switch off at maybe 18.00 and switch back on at 07.00 would save them being on all night and using all the energy this entails.*

ENVIRONMENTAL IMPACT OF INTELLIGENT SYSTEMS

Global warming is a fact of life and the amount of energy we consume can only make this worse. Therefore, anything that can be done to reduce our energy consumption will reduce the impact on the environment. Intelligent systems have been designed to reduce this impact. We are going to look at three ways:

1. Heating systems
2. Traffic Control
3. Car management systems

1. *Heating Systems*

Over the past couple of years, heating systems have become more intelligent to try to save energy and save the customer money. Some of the ways this is being done are:

- **Knowing when the house is empty**
  Some intelligent systems track the occupancy of the house by the location of the occupier's smartphones. If all the smartphones are 'out of the house' then it can lower the temperature of the house. If any of the smartphones start moving toward the house (using the phones GPS) then the heating can be increased; the closer the smartphone gets to the house the nearer it will be to the desired temperature.

- **Smart climate assistant**
  Some intelligent heating systems can be linked via the Internet to the weather forecast. If a very cold spell of weather is forecast then the heating can automatically be increased (or the time it is on extended). Similarly if a very warm spell is forecast then the temperature can be lowered or the system switched off all together.

- **Remote control of the heating system**
  Many intelligent heating systems now allow you to control your heating via your smartphone. For example, if you are going to be delayed at the office, what is the point of heating an empty house? By using your smartphone you can override the controls and tell it to switch on the heating later.

- **Zoning areas of the house**
  Different areas of the house are used more or less frequently, so what is the point of having them all at the same temperature? For example a spare bedroom may only be used once a month so could be set to a lower temperature.

All of the above should reduce the amount of 'wasted'energy our heating systems use therefore reducing the impact our heating systems are having on the environment.

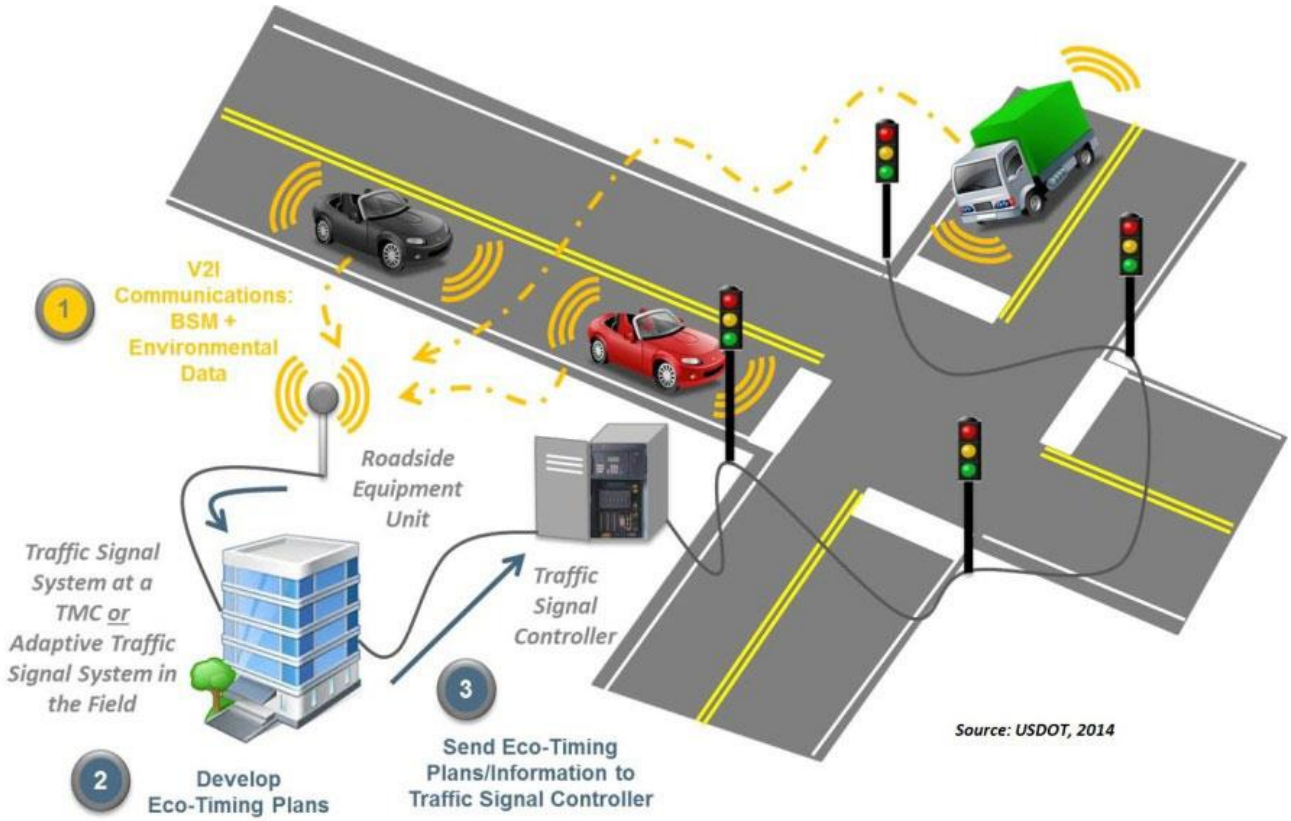
2. *Traffic Control*

A study in 2016, showed that the average motorist spends just over 44 hours per year sitting at red traffic lights. That is nearly two days! All of this time, the car engine is sitting running, using up fossil fuels and outputting noxious and polluting fumes.

Some of the ways intelligent systems are trying to reduce the environmental impact of this are:

- **Adaptive Traffic Signals**
  Adaptive traffic signals adjust the timing of their green light cycles to match current traffic conditions on the ground. They are constantly collecting data about approaching vehicles and creating new timing sequences to match them.

  Adaptive Traffic Signals utilise video cameras and sensors to collect information about the vehicles approaching an intersection. Software analyzes this information and creates a customized timing sequence in real time. The software communicates this sequence to coordinated signals up and down the corridor, so that they all function in sync with each other. This means that the traffic flows better and hence there is less pollutants given out so lessening the environmental impact.



- **Intelligent Routing Systems**
  Google reportedly paid $1billion for an app called Waze. Waze generates many of its maps by using GPS to track the movements of its nearly 50 million users. Users of Waze share "information about slowdowns, speed traps and road closures, allowing Waze to update suggested routes in real time. This should allow for less hold-ups due to accidents, traffic jams, roadworks etc and hence reduce wasted energy and pollutants.

  There is some talk of Waze being integrated into Google's driverless cars therefore allowing the cars to take the most economic route.

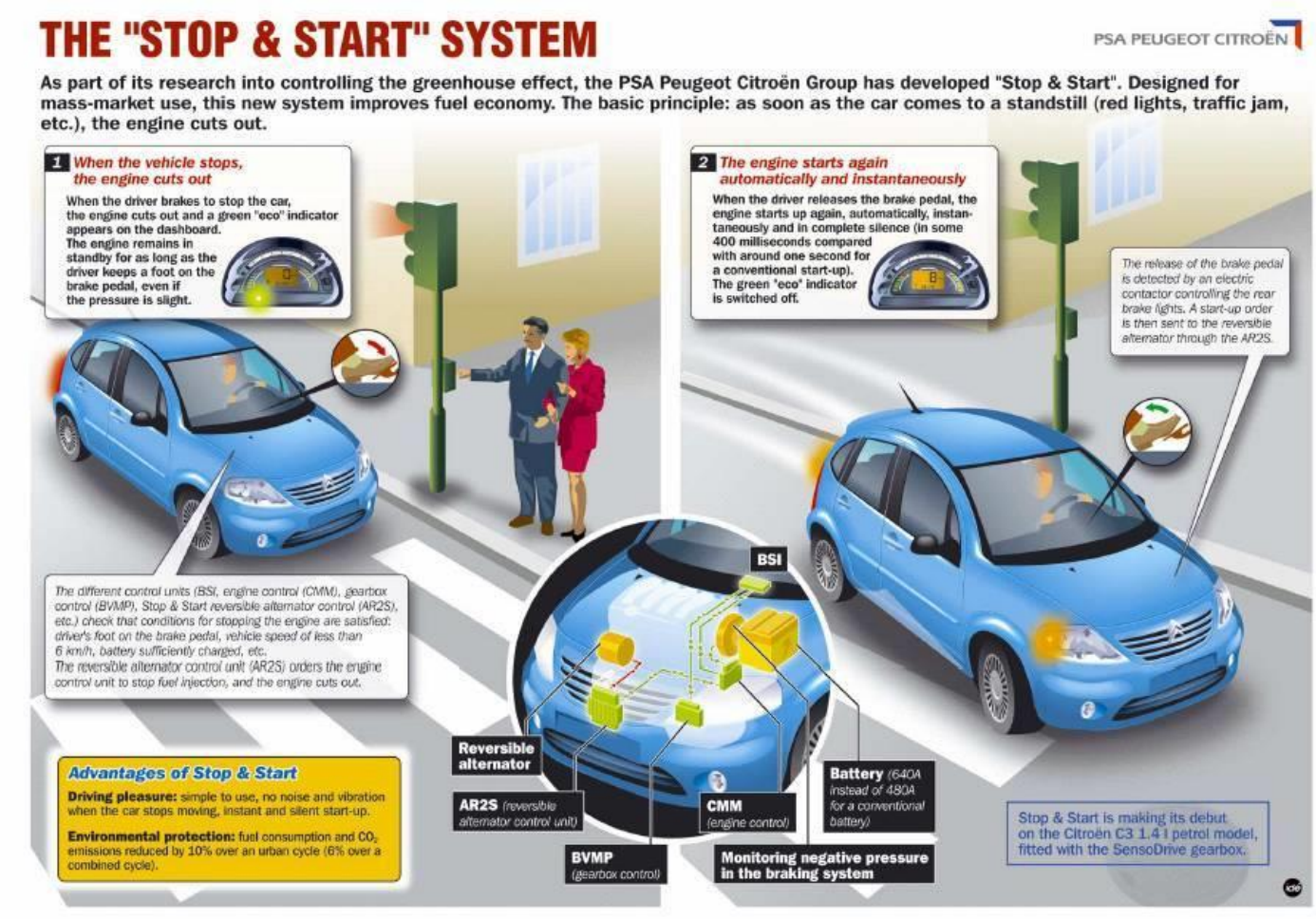
- **Driverless Cars**
  Cars consume much more fuel and hence give out more pollutants when they are driven erratically. Using high acceleration and severe braking at the last minute, uses a lot more energy than a gradual acceleration and deceleration. Unfortunately, at the moment this is controlled by the driver. However, driverless cars are set to become available in the near future. These cars will have an intelligent system that will ensure that they gradually accelerate and decelerate (except in an emergency) which should reduce the energy consumed and hence reduce the impact on the environment.

3. *Car Management Systems*

A number of manufacturers are using car management systems to try and reduce the impact of the car on the environment.

Some of the ways intelligent systems are trying to reduce the environmental impact of this are:

- **Intelligent Start Stop Systems**
  When a car sits at traffic lights with the engine idling, it is using fossil fuels and emitting polluting fumes. Car manufacturers have created a system called the 'Intelligent Start/Stop System' whereby when the car is in neutral and the clutch engaged the engine will automatically be switched off. When the clutch is disengaged then the engine automatically starts again. This system is estimated to be reducing fuel consumption by between 3% - 10%.



- **Engine Control Units**
  Engine control units are becoming more common in cars as manufacturers try to reduce emissions from their cars and improve energy efficiency. A variety of sensors including temperature and manifold air pressure sensors ensure an optimized air-fuel mixture for more efficient combustion. A more efficient combustion means less fuel used and less pollutants.

SECURITY RISKS AND PRECAUTIONS

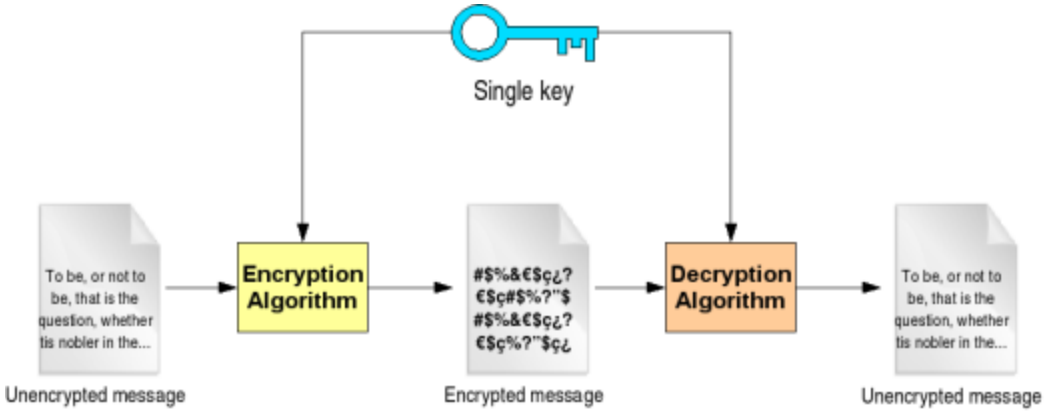
NATIONAL 5 REVISION

A firewall protects against people trying to hack into your computer. It does this by checking when an external computer tries to access your computer, the firewall examines whether it is allowed to access your computer. If it is, then access is given. If not then it is blocked.

A firewall can block access using either packet filtering or IP blocking.

Encryption codes the information so that if it is intercepted then they would not be able to make sense of it.

At the senders side the message is encrypted using a 'key' and at the destination end it is decrypted using a similar key.



COMPUTER MISUSE ACT

The Computer Misuse Act 1990 is designed to protect computer users against wilful attacks and theft of information. The act made it illegal to:

1. access computer material without permission.
2. access computer material without permission with the intent of committing further offences.
3. modify computer materials without permission

1. *Access computer material without permission*

A person is guilty of breaching this part of the act if it can be shown that the person has knowingly attempted to access someone else's computer materials (programs/data) without permission. Note: the attempt does not need to be successful, just attempting to access it is enough to be in breach of the act. Also, this does not need to be someone trying to guess your username and password, it can also include using software like keystroke loggers or spyware to gain access to computer material without permission. Someone found guilty of this would face up to 6 months imprisonment or a fine.

2. *Access computer material without permission with the intent of committing further offences*

A person is guilty of breaching this part of the act if it can be shown that the person has used data gained from someone else's computer to commit a further offence. For example, if by hacking someone's computer you gained access to their bank account details and passwords and used this to steal money from their account. Similarly, you are equally guilty if you pass the information onto someone else who uses the information to commit a further offence. Someone found guilty of this would face up to 5 years imprisonment and/or a substantial fine.

3. *Modify computer materials without permission*

A person is guilty of breaching this part of the act if it can be shown that the person has changed/deleted information on the computer without permission. For example, if a person hacked into a bank and the amount of money they had in the bank. This part of the act also includes the spreading of computer malware e.g. viruses or spyware which will install and copy itself on computers without permission.

Implications of Computer Misuse Act

There are implications both for individuals and businesses of someone gaining access to their computer materials illegally:

- Businesses losing income if the access shuts their e-commerce site down so they will not be able to make sales until the site has been completely checked to ensure that no malware has been installed.

- Businesses may lose their good reputation as if it is made public that they have been hacked and clients may not believe they can be trusted any more. Would you put your money into a bank that was hacked regularly?

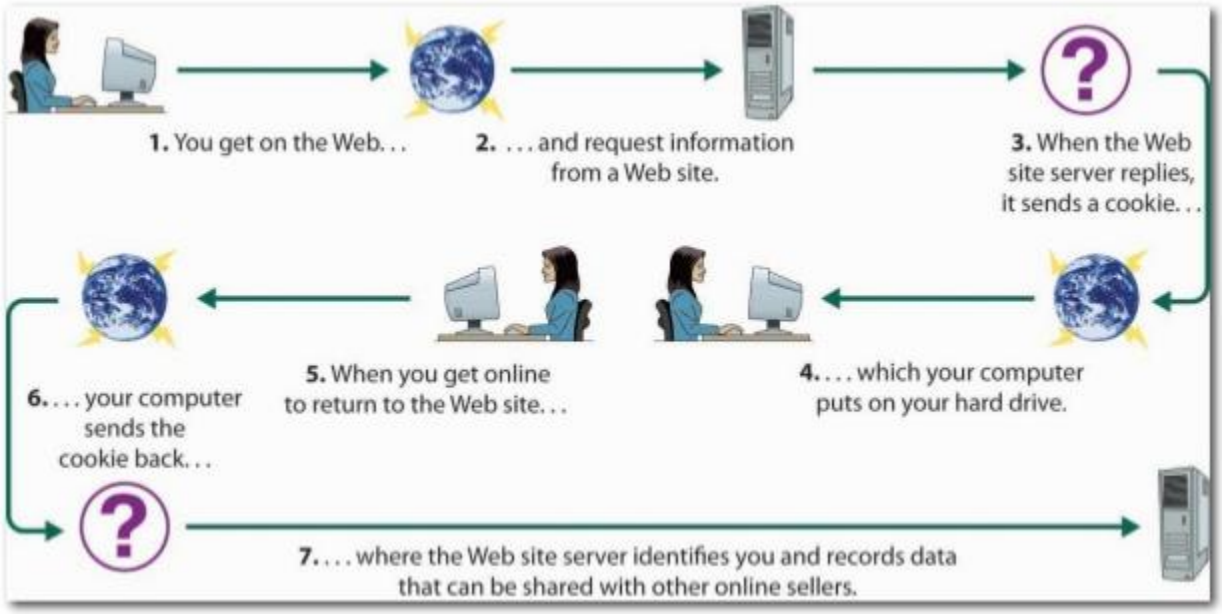
- There are significant costs associated with improving security to prevent further attacks. This may involve bringing in computer security experts.

- There is a risk of viruses or malware lying undetected but could send information to hackers/criminals.

- The work of the business may not be able to continue. In May 2017, hospitals and doctors surgeries in England and Wales found a message saying that all their files had been locked and would only be unlocked if they paid $300. Life threatening patient operations and appointments had to be cancelled causing chaos across the NHS.

TRACKING COOKIES

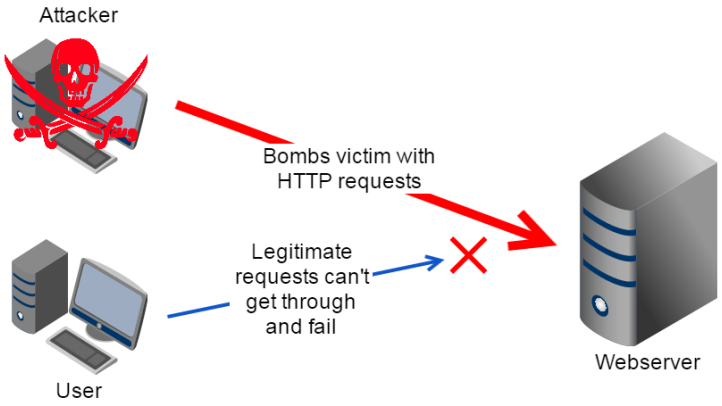
Tracking cookies are a specific type of cookie that is used to identify users and possibly prepare customized web pages for them. When you enter a web site using cookies, you may be asked to fill in some information for example search criteria. This information is stored on your computer as a cookie file (a small text file). The next time you go to the same web site, or a website that can access the tracking cookies, your browser will send the cookie to the web server. The server can use this information to present you with custom web pages.



Tracking cookies are not harmful and don't pose a security risk like malware, worms, or viruses, but they can be a privacy concern as they store and pass information to other websites about websites you have been visiting and information you have been entering into them.

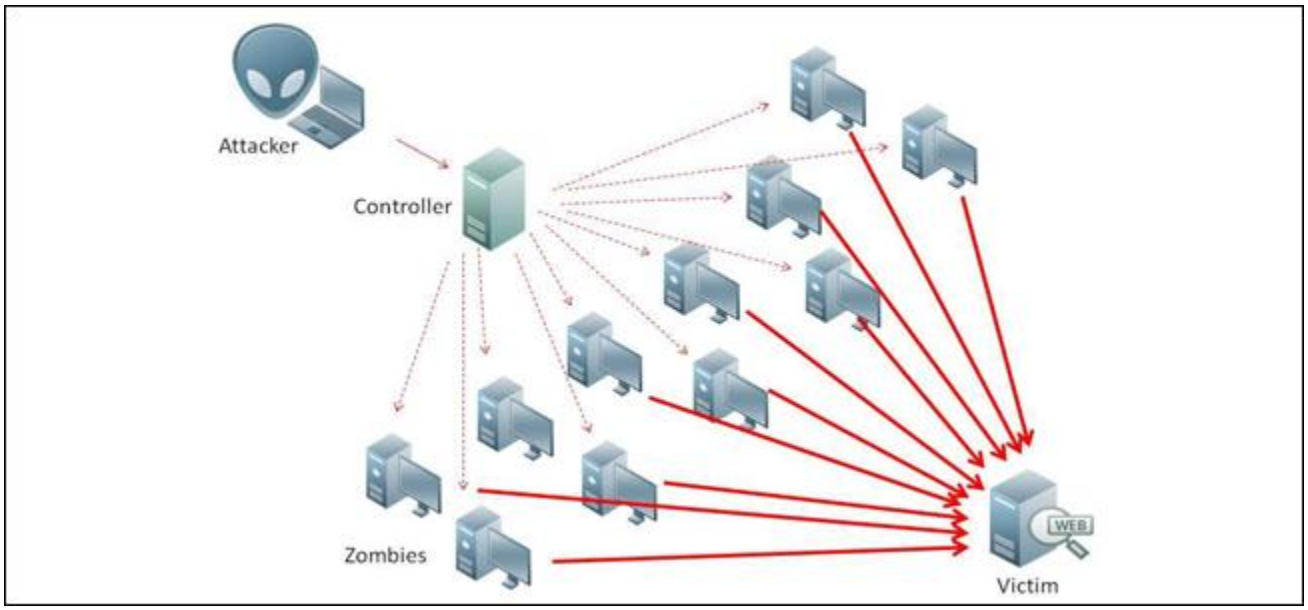
DENIAL OF SERVICE ATTACKS

A denial of service (DoS) attack is a cyber attack that involves flooding a web server with a large number of requests so the webpages stored on it become unavailable to legitimate users.



As can be seen from the diagram opposite, this type of DoS attack can be halted quite easily by blocking the attacker using a firewall.

To get round this, attackers are now using DDoS (Distributed Denial Of Service) attacks.



This is where a large number of slave computers (who may not even know they have this spyware installed on them) all send requests for information from the 'target server'. Because the requests are coming from thousands if not millions of computers, it is much more difficult to clock these attacks.

Implications of DoS attack

Symptoms	• ***Slow performance*** Due to the server being flooded with requests for information the server will be spending so much of its time servicing these requests that other requests e.g. access to a webpage or opening a piece of software will be extremely slow. • ***Inability to access*** At the extreme end, if the server is unable to cope with all these requests then it may crash or shut itself down. Both of these will mean that legitimate users will be unable to access the server.
Effects	• ***Disruption to users and business*** A report in 2014 surveyed a large number of companies about DoS attacks and the affect it had on their businesses. 39% of companies said that their server had been down for 1 hour or less. 16% selected between 1 and 4 hours and 6% experienced between 4-8 hours. Obviously if the main server is not available for this length of time there is severe disruption not only to customers who are maybe trying to access the company website, but also to company employees who are trying to get on with their work.
Costs	• ***Lost revenue*** The latest Neustar report on DoS attacks found that the average revenue loss of a DoS attack was about $250,000 per hour.  This could either be from customers not being able to buy goods from your website, or from employees not being able to carry out the organisation's business e.g. trading in stocks and shares.

Costs continued	• ***Labour in rectifying fault*** When a DoS attack is detected there is a responsibility on the business to put sufficient security precautions in place to ensure that it doesn't happen again. This can involve hiring security consultants, designing a new network architecture and buying new hardware and software; this can cost hundreds of thousands of pounds and upwards depending upon the size of the business. Also when a DoS attack occurs, there is also the worry that other malware may have been planted on the servers that will pass private information to the attackers. A huge amount of time will be spent checking the servers to ensure no malware has been planted.
Types of Fault	• ***Bandwidth consumption*** A smurf attack relies on misconfigured network devices that allow packets to be sent to all computer hosts on a particular network via the broadcast address of the network, rather than a specific machine. The attacker will send large numbers of IP packets with the source address faked to appear to be the address of the victim. The network's bandwidth is quickly used up, preventing legitimate packets from getting through to their destination. • ***Resource starvation*** The resources that are being starved are items like the computer's memory, hard disc space and even CPU processing time. For example, a disk space attack, is one in which an attacker is able to consume a particular resource until it is exhausted. For example, an attacker might continuously issue requests to your Web site to create folders or create users. If this occurs, you will eventually run out of disc capacity. Another example is a memory starvation attack is designed to force your Web site to consume excess memory. If an e-commerce site is the target, then an attacker can continuously add items to 'baskets' using a script that adds millions of line items so an attacker will eventually exhaust the available memory of the server, resulting in a DoS.

Types of fault continued	• ***Domain Name Service (DNS)*** A DNS server is a computer server that contains a database of public IP addresses and their associated hostnames, and translates those common names to IP addresses as requested. For example, to connect to the website www.lifewire.com the computer really needs to know its IP address 151.101.129.121. When you type in the web address in a browser the DNS server translates this into the IP address. A DoS attack can target the DNS server for a particular company meaning genuine clients when they enter the web address are unable to get it translated to the IP address and are therefore unable to access the website. A particularly notable DDoS attack on authoritative DNS servers was the attack on Dyn in October 2016. Attackers used a whopping 1.2 terabits per second of traffic to overwhelm Dyn's DNS server. Dyn's DNS servers couldn't respond to legitimate DNS queries under the load, which left Dyn's customers, including the New York Times and Twitter, unreachable.
Reasons	• ***Financial*** Criminal gangs use DoS attacks on companies and then tell them they will only stop the attacks if they pay them a certain amount. Because these attacks are slowing down or crashing their servers, some businesses choose to pay this 'ransom'. • ***Political*** DoS attacks are sometime used for political purposes. Examples are: o When Russia fell out with Estonia and Georgia a significant increase in the DoS attacks on those countries could be directly attributed to Russia. o When America imposed increased sanctions on North Korea, a large number of DoS attacks occurred on American companies that were traced back to North Korea. o In the lead up to the Russian elections in late 2007, the website for the dissident politician and well-known chess Grand Master Gary Kasparov and his political party were both hit with substantial DDoS attacks. Kasparov has been a very vocal

	counterpoint to the powers in Moscow, specifically former Russian president Putin's administration, for many years. During the attacks, Kasparov's site was inaccessible, and so was his political party's. o Most recently, in January 2016, the New World Hacking group claimed responsibility for taking down Donald Trump's website as they disapproved of some of his politics. o It is anticipated that the next major war between countries will involve 'cyber-war' where DoS and other types of attack will be involved to try and ruin the countries infrastructure. • ***Personal*** Sometimes DoS attacks take place for personal reasons: o Revenge, when an employee is made redundant they sometimes wish to take revenge on their employer and hence either carry out a DoS attack or pay for one to be carried out. o In hacking circles there is sometimes a level of 'Kudos' for bringing down a large server. These are sometimes known as 'Script Kiddies' due to the childish motivation of the attacker.

ENCRYPTION

With so much information being transmitted electronically, it is essential that the information be transferred safely and securely. One of the methods of doing this is to use encryption.

Public & Private Key Encryption (Asymmetric Encryption)

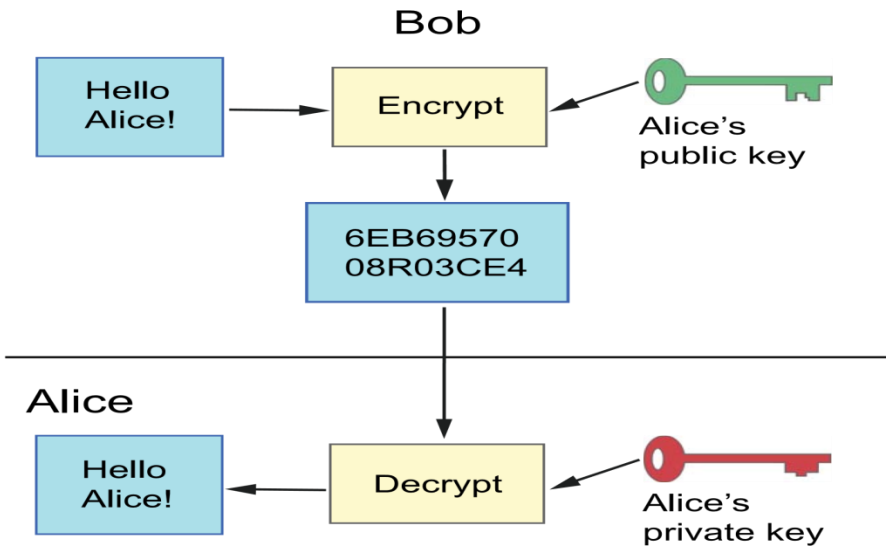
Public & Private key encryption (sometimes called asymmetric encryption) involves generating two keys, a public key and a private key. Both keys are mathematically linked using very large prime numbers. Both keys work as a pair.

- ***Public Key***
  The public key can be distributed to anyone who wishes to send you a message and they use this public key to encrypt the data.

  The public key can also decrypt data that has been encrypted with the private key.

- ***Private Key***
  The private key is known only by you only this private key can be used to decrypt data created by the corresponding public key.

In the example opposite, Bob wishes to send Alice an encrypted message. Alice sends Bob her public key which he uses to encrypt the message. He then sends the encrypted message to Alice who uses her private key to decrypt the message.



If Alice wished to reply, then she could encrypt the message with her private key and send it to Bob who can decrypt it with her public key.

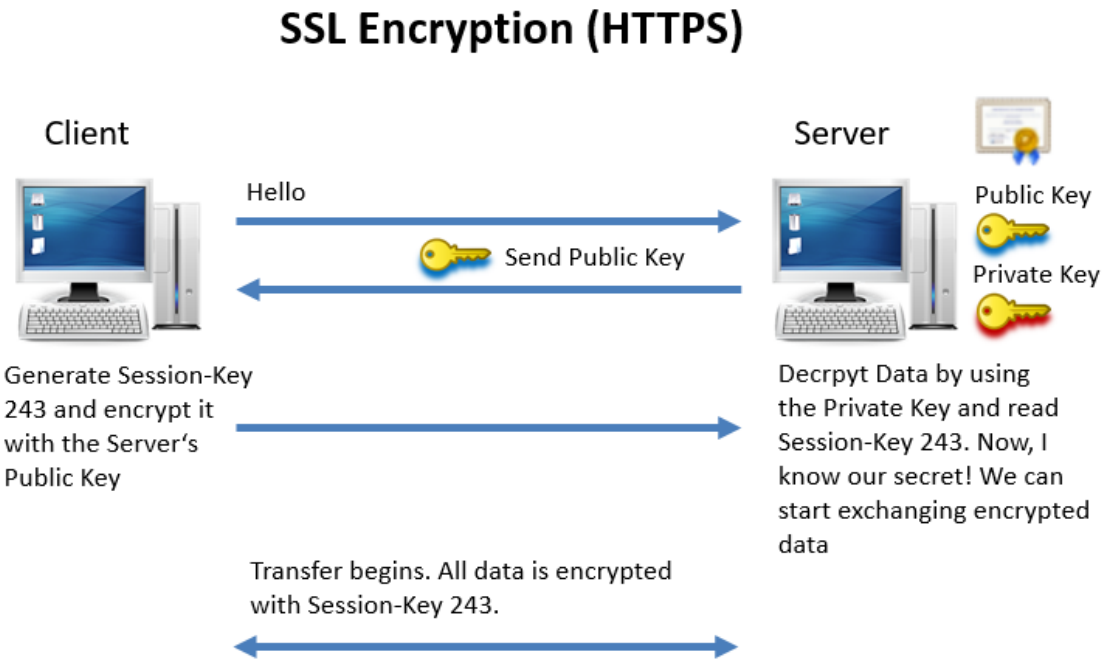
Secure Socket Layer (SSL) is a popular encryption system for secure websites. It operates by:

1. Your browser will be sent the website's public key - the private key remains on the website's server, so is still secure and cannot be intercepted.

2. Your browser, uses the public key to encrypt the data you are sending (for example your credit card details)

3. The data is sent back to the server - even if someone has intercepted the public key and your message they still cannot decrypt the message as they do not have the private key.

4. Once back at the server, the private key is used to decrypt the message.



Commonly 256-bit encryption is used. This has: 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936 (78 digits) possible combinations.

No Super Computer can crack this by brute force. Even if you use Tianhe-2, the fastest supercomputer in the world, it would take over 25 years to crack the 256-bit encryption.

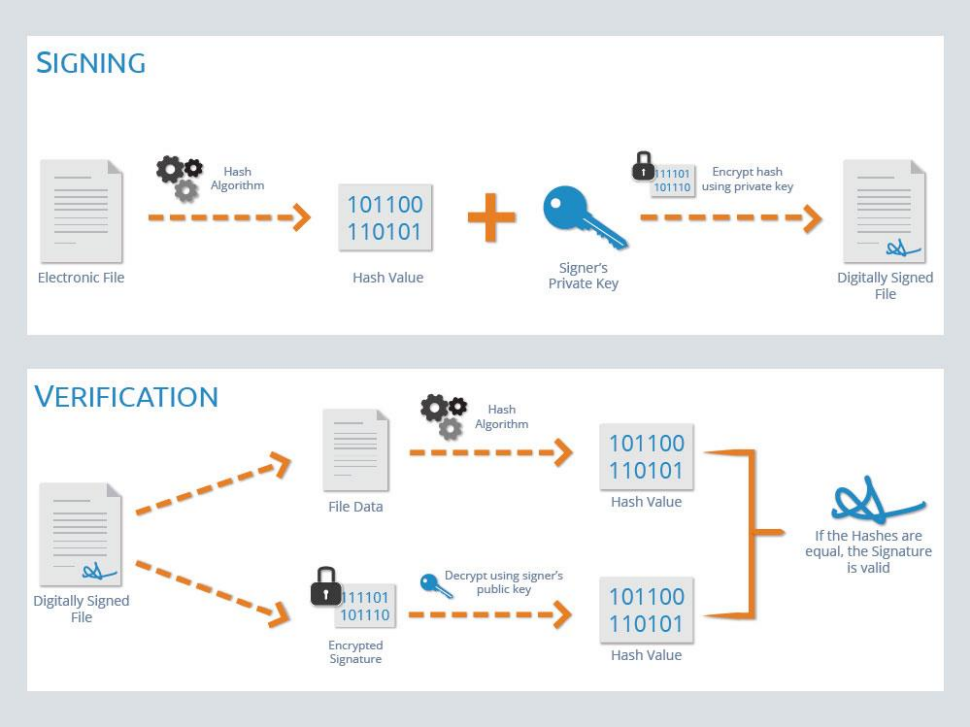
Digital Signature

The purpose of a digital signature is to authenticate the identity of the sender and ensure that the content has not been modified en route.

Digital signature are very difficult to forge and can automatically include a date and time. Digital signatures can be used as legal evidence that the message came from the person sending it and it has not been modified.

A digital signature is created by:

1. A mathematical value (called the hash total) is calculated from the unencrypted data. Because the hash total is calculated from the original message even the slightest change to the message would produce a different hash total.
2. The sender of the message encrypts the hash total using their private key and this encrypted total becomes the digital signature.
3. The digital signature is added to the message and the entire message (message + digital signature) is encrypted using the recipient's public key then sent to the recipient.
4. The recipient decrypts the message using their private key and decrypts the digital signature using the sender's public key.
5. The hash total is then recalculated on the message and if it is the same as the total in the digital signature then the recipient can be sure that the message is from the identified sender and has not been modified in any way during transmission.



DIGITAL CERTIFICATE

Hoax digital signatures can be created using a fake private key claiming to be that of a trusted individual. To get around this, a digital certificate verifies that a sender's public key is formally registered to that particular sender.

Digital certificates are issued by certificate authorities such as Verisign or Symantec. This certificate allows the holder to use the Public Key Infrastructure (PKI).

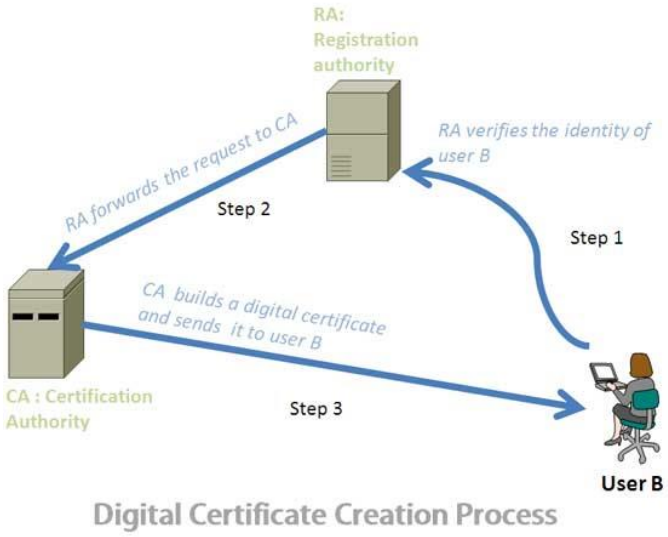
The digital certificate contains

- The certificate serial number
- The expiry date
- The name of the holder
- A copy of their public key
- The digital signature of the certificate authority so that the recipient can authenticate the certificate as being real and current.

Applying for a Digital Certificate

In order to obtain a digital certificate:

1. In order to obtain a digital certificate, for the first time, the applicant sends a request to the registration authority along with proof of their identity e.g. driving licence, business document etc. The registration authority verifies the applicant's identity and if satisfied then requests a digital certificate from the certificate agency on behalf of the applicant.



Digital Certificate Creation Process

2. The certificate authority creates the digital certificate using the applicant's public key and other identity information.

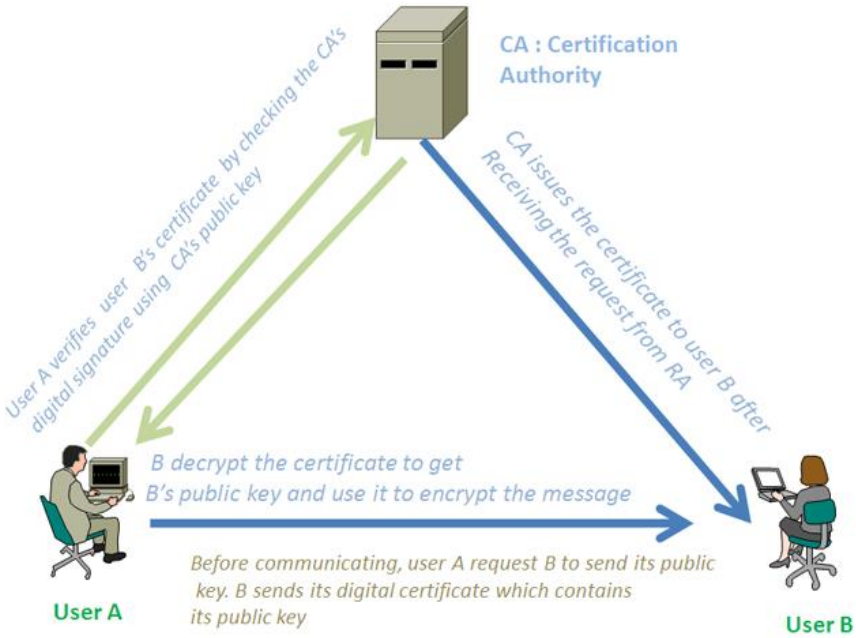
3. The certificate authority signs the certificate with its own private key in order to ensure the authenticity, integrity and non-repudiation of the digital certificate. Finally, the certificate authority sends back the certificate to the applicant, which can be used to establish secure communication.

Using a Digital Certificate

Using the previous process, User B has applied for and being granted a digital certificate. User A wishes to communicate securely with User B:

1. User A sends a request for user B's digital certificate to a certificate repository which is part of the certificate authority.

2. When User A receives user B's certificate it verifies it with the help of web browser by checking the digital signature of the certificate authority using its public key. Then user A uses user B's public key supplied by the certificate to encrypt the message.



Simplified diagram: Secure communication with digital certificate

3. When user B receives the encrypted message, it uses its own private key to decrypt the message.