Cambridge GCSE Notes
2210 Computer Science

Abrar Faiyaz Rahim, degrees pending

Introduction

What follows is my compilation of notes I used to get through my Ordinary Level GCSE exams, in the May-June session of 2025. I release all these notes to the public so as to help combat the tragic "coaching culture" surrounding GCSE exams. This set of notes is written to be used in accordance to the coursebooks published by Cambridge, and is of little use by itself.

My despiction of coaching culture arises from the fact that it ruins student life and to a large extent the academic potential of students. A typical student has school in the day and in the evening they are made to sprint to and from coaching centres, often multiple teachers for the same subject all as a result of peer pressure and they come back home at 9 or 10 at night. If they have been given homework, they must sacrifice their sleep to complete these assignments. Students cannot, as a result, study by themselves – ruining their potential.

There exist accessible resources which are more than enough for a candidate to ace their exams, without any aid from the financially-minded coaching sharks. One of the services provided by these teachers are "compiled notes", exchanged for money, further inflating the price of education. So, in retaliation I release these notes as open-source and free to distribute.

Yet coachings are not entirely evil, students who struggle in certain subjects may ask for the aid of teachers of those subjects but it is meaningless to go to a different teacher for each and every subject.

These notes are condensed, written in sequence of the Cambridge specifications.

Suggestions for readers

These notes are not at all stand-alone resources that will magically help you to get through your exams. I suggest purchasing and utilising the Cambridge coursebooks, and read the chapters from there before referring to these notes, especially if the topic in question is absolutely novel to you.

YouTube has excellent resources, lectures galore at your discretion, simply type in "GCSE" alongside whatever topic you need to watch the lectures on.

Lastly, for practice of questions, past papers both topically and yearly compiled are available for purchase at bookstores and for free online (topicals can be found on physicsandmathstutor.com).

Contents

1 Data Representation

1.1 Number systems

1.1.1 Computers and binary

The number system consisting of digits 0 through 9 is called the denary or decimal system (10 digits). Computers use another number system called binary, consisting of digits 0 through 1. This is done such that computers are able to pass the data through logic gates and can be stored in registers.

1.1.2 The binary, denary and hexadecimal systems

The number of digits in a number system is the base of that system; denary is base 10; binary is base 2; hexadecimal is base 16.

Conversions

From positive denary to positive binary:

1. Perform short division on given denary number, taking note of the remainders.
2. Write the remainders from bottom to top, resulting in the binary number.

From positive binary to positive denary:

1. Write the binary number with their *place powers*.
2. Sum the products of each binary digit with the place power, resulting in the converted denary number.
3. Write the remainders from bottom to top, resulting in the binary number.

From positive denary to positive hexadecimal:

1. Convert given number to binary
2. Split resulting binary number to four-bit parts.
3. Convert the four-bit binaries to denary.
4. 1 = 1; 2 = 2; ... 10 = A; 11 = B; 12 = C; 13 = D; 14 = E; 15 = F.
5. Arrange resulting digits side-by-side.

From positive hexadecimal to positive denary:

1. Convert each given hex number to denary using the index in step 4 of denary-hex.
2. Convert each denary number to binary.

3. Arrange the resulting four-bit binary pieces, producing binary result.

From positive hexadecimal to positive binary:

1. Convert to denary.
2. Convert to binary.

From positive binary to positive hexadecimal:

1. Convert to binary.
2. Convert to denary.

1.1.3 Uses of the hexadecimal system

The hexadecimal number system is used to make life easier for humans dealing with bare low-level computer code. Hexadecimal requires less digits, and are easier to compare with the naked eye. Data errors can be easier to find when looking at this shortened form of binary, hexadecimal.

1.1.4 Binary addition

To add two binary numbers, refer to the following:

- $0 + 0 = 0$.
- $1 + 0 = 1$.
- $1 + 1 = 10$. (the one is carried on)
- $10 + 1 = 11$. (the one is carried on)

Sometimes, the addition results in an extra bit, which **overflows** off. This is because computers have predifined limits to which it can store its numbers (16, 32 bits) and when a value outside this limit is returned, it is not stored and an overflow error occurs.

1.1.5 Logical binary shifts

When performing logical shifts, we simply move the bits of a binary number to the right or left depending on what is required. We "delete" and hence lose the leftmost (most significant) or rightmost (least significant) bit depending on the direction of the shift performed.

Shifting right means dividing by two.

Shifting left means multiplying by two.

1.1.6 Two's complement

Two's complement is a method used to represent negative binary numbers. We simply convert given denary number to binary (if need be), invert all the bits and add $(1)_2$ to the result.

1.2 Text, sound and images

1.2.1 Text

Text is converted to binary so that a computer can process it. It does so by converting each character into an integer, as defined in the **ASCII** standard (American Standard Code For Information Interchange) and subsequently into a binary number.

Unicode is another such standard, which allows a greater range of characters, in various languages, as a result it also requires more bits per character.

1.2.2 Sound

Sounds are composed of waves. When we record values of the sound, we do so at set intervals, this process is called **sampling**. The more samples taken per unit time, the more accurate the sound recorded will be, i.e., higher the **sample rate** the greater the sound quality.

The sound values, which are usually denary numbers, can be converted to binary and stored into a computer.

The **sample resolution** is the number of bits allocated per sample value. So, the larger the sample resolution, the more the amount of digits that can be stored into a file. Thus, the higher the sample resolution, the higher the sound quality.

The file size of a sound file increases, with increased sample rate and sample resolution, that means storing high quality sound requires more space that low quality sound.

1.2.3 Images

An image is composed of **pixels**. The computer stores these pixels by processing them to binary, by assigning a binary number to a certain colour.

The **resolution** of an image is the number of pixels stored in it. Usually in the format: width $\times$ height.

The **colour depth** of an image is the number of bits allocated for each pixel of the image. Higher the colour depth, the more the number of colours that can be displayed.

Higher quality images result in larger file sizes as resolution and colour depth are large.

1.3 Data storage and compression

1.3.1 Measurement of data storage

- Bit: 1 or 0. Smallest possible data measurement.
- Nibble: 4 bits.
- Byte: 8 bits.

- Kibibyte (KiB): 1024 Bytes.
- Mebibyte (MiB): 1024 Kibibytes.
- Gibibyte (GiB): 1024 Mebibytes.
- Tebibyte (TiB): 1024 Gibibytes.
- Pebibyte (PiB): 1024 Tebibytes.
- Exbibyte: (EiB) 1024 Pebibytes.

1.3.2 File size calculation

To calculate the file size of an image, find the product of the image's width, height, colour depth

For the sound's file size, multiply the sample rate, sample resolution and soundtrack length.

1.3.3 Compression

Files can be compressed to:

- Reduce storage space needed.
- Less transmission times among devices.
- Quicker upload and download times.
- Requires less bandwidth for file transmission.

Compression is of two types:

1. Lossy: Reduces file size by permanently reducing colour depth, resolution, or sample rate.
2. Lossless: Reduces file size without permanent loss of data, using Run Length Encoding (RLE). RLE groups similar data together and hence some file space can be saved.

2 Data transmission

2.1 Types and methods of data transmission

2.1.1 Packets and transmission

When data is transmitted from one device to another, it is organised into packets. A packet consists of three parts:

- Header: Consisting of three parts again: destination address, packet number and originators address.

  - The destination address is an Internet Protocol (IP) address which is a unique identifier address for every computer connected to the internet.
  - The packet number assigned to a packet helps the recieving computer reorder and organise the data sent, because often data may be sent out of order.
  - The originators address too is an IP address. It is that of the device from which data has been sent. It helps to trace origin of transmitted data.

- Payload: Consists of the actual data being sent.
- Trailer (Footer): Consists of data for any error detection system, and the data to signal to the reciever that this is the end of the packet.

Data is transmitted across a network (the internet for the majority of cases). Networks consist of routers. From one device to another, there exist multiple connected routers amongst whom there exists multiple paths whicch data packets can take. The routes are decided by the routers themselves. Packets may arrive out of order as a result but the packer number stored in the header helps the reciever reorder the recieved data. This is the process of packet switching.

2.1.2 Methods of dataa transmission

There are two methods of data transmission regarding the volume of data transferred:

- Serial: Data is transmitted along a single wire a bit at a time. Sequencec is maintained, very little interference is likely and cheaper for manufacturer and consumer because only requires one wire.

  However, data transmission is very slow and start and stop bits must be sent additionally.

- Parallel: Data is transmitted along multiple wires, multiple bits at a time. Data transmission is quicker, because of the sending of multiple bits at one time. No need for conversion for transmission across networks as computers use parallel transmissions internally.

  However, the bits may arrive out of order and skewing is a risk. Interference is likely and errors may arise. Expensive due to more wires required.

There are three methods of data transmission regarding the direction of data transferred:

- Simplex: Data is transferred in one direction only.
- Half-duplex: Data is transferred in both directions, not at the same time.
- (Full-)Duplex: Data is transferred in both directions at the same time.

2.1.3 The universal serial bus (USB) interface

The USB interfaec inclcudes the port, cable, connection and device. Data transmission, here is a special type of serial which allows high speed transmissions.

The USB interface is simple and connections can only be made in one way, less errors in onnecting devices are likely. The speed of data transfer is quite high. It is the industry standard so almost all devices are equipped with a USB port. When USB devices are connected, required drivers for the devices are automatically detected and downloaded. It does not need its own power source and can be used to charge devices.

The length of a USB cable is limited to a maximum of five metres. Transmission is quick yet not as quick as ethernet.

2.2 Methods of error detection

2.2.1 Necessity of error checking

Errors may occur as a result of interference during transmission, consisting of loss, gain and change of data being transmitted.

2.2.2 Processes to detect errors

These errors can be resolved in the following ways:

- Parity check: Given data is said to have even or odd parity. Bytes of data are sent with a parity bit, which is determined by the data itself. If the number of ones in the binary data is even and the parity is even, the parity bit will be one, otherwise zero. Same stands for odd parity.
- Checksum: A calculated value is transmitted with transmitted using a certain method. The reciever then uses the same method to calculate the value itself. If the transmitted and calculated values match, the data is error-free, otherwise it is corrupt.
- Echo check: Recieved data is sent back to the sender, who compares it with original data. If datas match, no error. Otherwise data is sent again.

2.2.3 Check digits

Check digits are identical to checksums but the the result of the generating algorithm is in a single digit. ISBN (International Standard Book Numbers) use check digits and so do barcodes.

2.2.4 Automated Repeat Queries (ARQ)

ARQs work in the following sequence:

1. Data is sent to reciever.
2. Reciever checks errors.

3. If data free, send positive acknowledgement to sender.
4. Otherwise send negative acknowledgement and sender re-sends data.
5. If no acknowledgement is sent beyond the timeout limit, sender sends data again.
6. Without acknowledgement, data is sent for a set number of times.

2.3 Encryption

2.3.1 The need for data transmission

Data needs to be encrypted so as not to lose sensitive data to potential hackers.

The original data is called the plaintext, having used an encryption algorithm, usually with an encryption key, a ciphertext is formed. This ciphertext is then sent across the network and some method of data decryption is used by reciever.

2.3.2 Methods of data encryption

Data can be encrypted in two ways:

1. Symmetric: Data is encrypted and decrypted using the same encryption key which is send along with the data itself. Vulnerable method as encryption key can also be compromised.
2. Asymmetric: Data is encrypted with the senders public key, decrypted with public key. This is the safer method as compromise is unlikely with only public key.

3 Hardware

3.1 Computer architecture

3.1.1 The central processing unit (CPU)

It is responsible for the process of data inputted into the computer to turn it into an output. A microprocessor is present in embedded systems and is an integrated circuit which is able to perform many of the functions of a CPU.

3.1.2 The Von Neumann architecture

The Von Neumann architecture consists of three stages in a cycle: fetch, decode and execute.

- Fetch:
    1. Inputted data, instructions and data from hard drive are initially stored and put into the RAM (Random Access Memory).

2. A register called the PC (Program Counter) stores the address of the next instruction to be processed. The address is the next location of RAM.
3. When an instruction is to be processed, the address from the PC is brought into the MAR (Memory Address Register). The address bus is used for the movement of registers.
4. Using the address stored in the MAR, the address bus retrieves the data at the address in the RAM, bringing it back into the MDR (Memory Data Register) using the data bus.
5. Once the MDR recieves the data, which is the next instruction to be processed, this data is sent to the CIR (Current Instruction Register). The transfer is done by the data bus.
6. This is the end of the fetch stage, the CIR is part of the CU (Control Unit) which is responsible for the second stage: decode.

- Decode:

  1. Using an instruction set, the CU decodes the instruction stored in the CIR.
  2. This is the end of the decode stage, now the execute stage can begin.

- Execute:

  1. Here actions required for carrying-out of instructions are done.
  2. Calculations are done by the ALU (Arithmetic Logic Unit). The ALU has a register called the ACC (ACCumulator) where any temporary values needing to be stored are stored.

The stages in the fetch-code-decode cycle are coordinated by signals transmitted through the control bus.

3.1.3 CPU Performance

CPU Performance is controlled by three main factors: number of cores, clock speed and cache.

- Cores: The more the number of cores the better the performance as more fetch- decode-execute cycles can run simultaneously.
- Clock speed: A CPU contains an internal clock which controls speed of processing of instructions. Using overclocking, CPU can process more instructions quicker but it can cause overheating.
- Cache size: Cache is a type of storage inside and hence near the CPU. The more instructions stored in cache the better as it takes less time than fetching instructions all the way from RAM.

3.1.4 Embedded systems

Embedded systems are essentially small computers that are built to do a very specific task. Examples include the systems embedded into domestic appliances (microwaves, fridges, etcetera), vending machines, security systems or lighting systems. They use microcontrollers in place of a CPU and usually lack some parts of the Von Neumann architecture.

3.2 Input and output devices

3.2.1 Input devices

An input device is that which allows any entering of data into a computer system, including text, image and sound.

Required input devices:

- Barcode scanner: Used to scan data encoded into a barcode (a linear image consisting if dark and light lines).
- QR (Quick Response) code scanner: Used to scan data incoded into a QR code (an image consisting of dark and light squares arranged in a matrix pattern).
- Digital camera: Used to take digital images of surroundings.
- Keyboard: Used to type in text into a computer system.
- Microphone: Used to input sound data into a computer system.
- Optical mouse: A pointing device which uses a CMOS (Complementary Metal Oxide Semiconductor) to detect movement and maps that movement into the pointer on the screen.
- Touchscreen: Can be of three types: capacitive, resistive and infrared:
  - Capacitive: Voltages are produced at all four corners of the screen, any contact by finger or stylus results in change in electric field produced, position of contact can then be calculated.
  - Resistive: Consists of two layers, when pressure is applied, the layers come into contact, completing a circuit and position of contact is calculated.
  - Infrared: Infrared light beams are shot across thes screen in an X-Y pattern. When a finger or stylus contacts the screen, the light rays are blocked and the position of contact can easily be calculated.
- 2D and 3D scanners: 2D scanners are used to scan what is printed onto a piece of paper, a document. This is done to digitise the document.

  3D Scanners scan and produce a 3D image of a given object. This can be used in CAD (Computer Aided Design) circumstances.

3.2.2 Output devices

An output device is that which allows for the result of data processing to be understood by humans.

Examples are:

- Actuator: An actuator is a mechanical or electromechanical device such as a relay, solenoid or motor. They are needed to start/stop and open/close mechanical parts.
- Digital light projector (DLP): Uses millions of micro-mirrors on a small digital micromirror device (DMD).

  Gives high contrast ratios, lasts longer, is quieter, gives no issues lining up images, smaller and lighter than LCD projectors, do better in dusty or smoky atmospheres.

  Shadows arise with moving images, lack grey components, colour saturation (intensity) not as good as LCD projectors.
- Liquid crystal display (LCD) projector:

  1. White light is split into red, green and blue by dichromatic mirrorrs.
  2. These three groups are reflected by chromatic-coated mirrors into another set of mirrors;
  3. Lastly they are reflected into a special prism which outputs the image.

  Give sharper images than DLP projectors with better saturation, less heat is generated and are more efficient.

  Contrast ratios are worse, do not last long, degrade over time (organic nature).
- Inkjet printer:

  1. Document sent to printer driver which ensures document format.
  2. Check to see if printer is busy.
  3. Data is sent to the printer buffer (temporary memory).
  4. The print head moves laterally across the paper printing text.
  5. Advanced vertically forward and repeated until page is printed.

  Piezoelectric inkjet printers used charged crystals to eject ink onto paper.

  Thermal bubble inkjet printers use tiny resistors to produce heat, form ink bubbles which is then ejected onto paper.

  Small ink cartridges and paper trays make it such that few colour images are feasible with inkjet printers.
- Laser printer:

1. Same as inkjet.
2. Same as inkjet.
3. Same as inkjet.
4. Positively charged ink sticks to negatively charged printing drum.
5. Ink droplets stick to negatively charged paper.

Can print lots of documents in high quality very quickly, can hold a large amount of paper and large amounts of ink.

- Light emitting diode (LED) screen: Composed of tiny LEDs, which are either red, green or blue. Varying current sent to each LED produces variation in base colour brightnesses, producing colours.
- Liquid crystal display (LCD) screen: Composed of tiny liquid crystals, making up a matrix of pixels affected by changes in electric fields. LCDs themselves do not produce any light and so they are backlit using LEDs.
- Speaker: Digital (stored) data of sound is passed through a DAC, resulting data is passed through an amplifier and subsequently a varying current is made to pass through a solenoid which subsequently makes a plastic/paper cone move producing sound waves in the air.
- 3D printer: Builds up layers, horizontally and then vertically to produce a solid object. Uses powdered resin, metal or ceramic. Can be used for prosthesis, reconstructive surgery, aerospace, art, parts no longer in production.

3.2.3 Sensors

These are input devices which read things from their surroundings and convert them to digital data using an ADC.

Required sensors:

- Acoustic: Microphones that convert sounds into electric signals/pulses.
- Accelerometer: Uses a piezoelectric cell whose electric output changes with change in velocity of that being observed.
- Flow: Measures rate of flow of a moving liquid or gas based on the amount of substance passing over the sensor.
- Gas: Uses various methods, produces varying output depending on gas present.
- Humidity: Measures the amount of water vapour in a sample of air.
- Infra-red: Uses a detector which detects infra-red beam, if broken, electrical signal is changed.

- Level: Ultrasonics are used to check how high a liquid is in a container.
- Light: Photoelectric cells are used which produce an output depending on the presence and intensity of light.
- Magnetic field: Output changes according to change in magnetic field sensed.
- Moisture: Measures water level in samples using electrical resistance.
- pH: Measures acidity using changes in voltages.
- Pressure: A transducer that generates a different current based on pressure applied.
- Proximity: Detect presence of any nearby object.
- Temperature: Uses signals that change as temperature changes to output signals that change as temperature changes.

3.3 Data storage

The memory and storage devices of a computer are in two parts, primary and secondary.

3.3.1 Primary storage

Primary storage devices are those that can be accessed directly by the CPU, these include Random Access Memory (RAM) and Read Only Memory (ROM).

RAM is used to temporarily store some data, such as file data in use and yet to be saved. RAM is volatile meaning all contents of RAM is lost as soon as the computer is turned off. RAM can be read from and written to.

ROM consists of the BIOS, cannot be written to and are very little in amount. Data is non-volatile, i.e. permanent.

3.3.2 Secondary storage

Secondary storage is not accessed directly by CPU and is used for more permanent storage.

3.3.3 Magnetic, optical and solid-state storage

Magnetic memory is stored on a magnetic disk, using tracks and sectors on the disk. Data is read and written using electromagnets.

Optical storage (DVD, CD) uses a laser to dig physical pits and lands onto disks, which can be interpreted as data.

Solid-state or flash memory uses NAND and NOR technology to store electric pulses as memory, transistors are used as control and floating gates.

3.3.4 Virtual memory

When a computer is about to run out of RAM space, it allocates some memory to secondary storage so as to avoid a system crash, where the memory is located is called virtual memory.

3.3.5 Cloud storage

Data is stored on remote servers, so that users can access this data any time they want.

Allows for backups to be made, almost unlimited capacity, and there is no need to be carrying a whole storage device on the user's person all the time.

Data stored, however can be hacked. Data stored can also be lost by the cloud company itself. Large amounts of storage is expensive. Internet speed can affect user experience.

3.4 Network hardware

3.4.1 Network interface card (NIC)

To be part of a network, a device requires a NIC.

3.4.2 Media access control (MAC)

The NIC holds a Media Access Control (MAC) address which is unique to that NIC and is assigned by the manufacturer at the time of manufacture. It consists of the manufacturers identification code followed by the devices unique identification code in the following format:

NN-NN-NN-DD-DD-DD

where N is the manufacturer code and D is the device code. The MAC address is usually in hexadecimal.

3.4.3 Internet protocol (IP)

IP addresses are unique addresses assigned by the network onto devices that are part of the network, each IP of a device to a network is unique inside of that network.

Dynamic IPs are those where the IP changes each time the device connects to the network. Static IPs are those where the IP stays the same, even after disconnection and reconnection to the same network.

IPv4 was the initial version of the protocol, consisting of four eight-bit numbers seperated by periods. An example may be:

256.123.145.27

IPv6 is the newer version using 128-bit numbers of eight groups seperated by colons. Because of the size of each group of an IPv6 address, it is represented in hexadecimal:

A8FB:7A88:FFF0:0FFF:3D21:2085:66FB:F0FA

3.4.4 Routers

Routers are involved in packet switching, and they identify different devices using the differences in IP addresses.

4 Software

4.1 Types of software and interrupts

4.1.1 System and application software

In general, there are two types of software: system and application.

- System: Consists of the Operating System (OS) and utility software (compilers, drivers, anti-viruses etc), required for device usage.
- Application: Consists of services required by the user: word processors, video editors etc.

4.1.2 The role and functions of the OS

The OS's job is to manage the user's files, handle system interrupts and it provides an interface between the software and hardware of a device. It manages drivers required for peripheral input devices, it's the OS's job to manage the multiple tasks being done by the user and the priority of those tasks. It is the OS's job to manage memory allocation. It is upon the OS that application software runs, and the OS provides security consisting of anti-viruses. It also manages the user's accounts.

4.1.3 Hierarchy dependencies

The bootloader or the firmware runs diretly on the hardware. It is upon the firmware that the OS runs on which run applications.

4.1.4 Interrupts

Interrupts are basically signals to the processor. Every interrupt has a priority level and interrupts are handled by the creatively named interrupt handler (IH). The IH procedure follows:

1. After an FDE cycle is done, the system checks for any generated interrupts.

2. It compares the priority of the interrupt to the next task to be processed, if it is the next step is processed otherwise step 7 is executed.
3. Stores the less process with inferior priority.
4. Checks what sent the interrupt.
5. Calls the relevant interrupt service routine (ISR), which is a procedure that handles the interrupt.
6. When the ISR is done it goes back to the FDE cycle that was stored away.
7. Execute the the FDE cycle.

Interrupts are generally of two types: software and hardware. Examples follow:

Software:

- Division by 0.
- Two programs accessing the same location at the same time.
- Input request.
- Output request.

Hardware:

- Data input (key pressed).
- Mouse moved.

4.2 Types of programming language, translators and integrated development environments (IDEs)

4.2.1 Types of programming language

Programming languages are generally seperated into two categories: high-level and low-level.

High-level languages

These are languages which have statements consisting of English words. Examples of such languages are Python, VB.Net and Java. An example of a statement in a high-level language is:

```
int age = 16;
String username = "Abrar";
```

A program written in a high-level language is "portable" in the sense that the program code can be executed on any computer regardless of what device the code was written on.

Low-level languages

Low-level languages are generally of two types once again: machine and assembly language.

Machine language consists of 1s and 0s that only the computer can read, and high-level languages are translated into machine code before it can be executed. Machine code is non-portable because code that executes on one device may not on another because of the differences in manufacturer and OS formats.

4.2.2 Assembly language

Assembly language uses mnemonics such as LDD (load) ADD (add) etc. It's still human readable but less so than high-level languages. It allows very close communication to hardware, but lots of statements need to be written for a very simple instruction. Example:

```
LDD 8x7917f
ADD 1
STO 8x7919f
```

4.2.3 Translators

To execute program code the code must be translated down into machine code, which is done by means of usage of translators.

Compilers

The compiler goes through the whole program code, reporting any and all errors before producing an executable file. If errors are found they are shown to the programmer and no executable file is produced.

Interpreters

These are translators that translate and execute the program code line-by-line. If errors are found the translation process is stopped and the error is reported, as a result not all errors are reported at once.

4.2.4 Compilers and interpreters in context

Compilers are useful when one is done with building a program, as an executable file will then be produced. Interpreters are not suitable because interpreter software will be required to run the code alongside the actual code making it difficult to distribute.

Interpreters are useful while building a program, as errors pop up as the program is being executed. Compilers are unsuitable during the building process because all errors must be fixed before execution.

4.2.5 Integrated development environments (IDEs)

IDEs are used to write program code. They are complex software that provide all the utilities needed by a programmer. Including:

- Code editors: Used to edit the code itself.
- Run-time environment: Used to see the output of the code.
- Translators: Discussed in the previous sub-subsection.
- Error diagnostics: Tells you where and why an error is occurring.
- Auto-completion: Suggests the ending of a command which the user is typing.
- Auto-correction: Changes what the user wrote to what the user meant.
- Prettyprint: Colours different keywords differently for ease of the programmer.

5 The internet and its uses

5.1 The internet and the world wide web

5.1.1 What's the difference?

The internet consists of the infrastructure, i.e. the cables and routers and all the devices that are used to connect the devices connected to each other. The network itself is the internet, in this case its called a Wide Area Network (WAN) and the wide area in question is the whole world.

The world wide web, is the collective name given to the websites and webpages available for access through the internet.

5.1.2 Uniform resource locator (URL)

A URL is the unique text-based address for a website on the internet. It's typed into the address bar of a web browser. It consists of three parts: protocol (HTTP or HTTPS), the domain name (website name, youtube, netflix, etc) and the webpage name (the name of the page inside the website itself) in the following format:

protocol://www.domain-name/web-page-name

5.1.3 HTTP and HTTPS

HTTP stands for Hyper Text Transfer Protocol and it is by this protocol that webpages are transferred across the internet to web browsers. HTTPS is simply Hyper Text Transfer Protocol Secure and it is used to securely transfer these webpages, by use of digital security certificates.

5.1.4 The web browser

The primary function of a web browser is to retrieve webpages (the process is shown in the next sub-subsection), and to render and display those webpages to the user. All webpages are written in the Hypertext Markup Language (HTML) alongside Cascading Style Sheets (CSS) and some active scripts written in languages such as JavaScript. Modern webpages provide functions such as:

- Bookmarking and storing favourite websites.
- Recording user's browsing history.
- Allowing use of multiple tabs to browse multiple places simultaneously.
- Storage of cookies.
- Provision of navigation tools.
- Providing an address bar.

5.1.5 The process of location, retrieval and display of a webpage

1. The user types in the desired website's URL into the browser's address bar.
2. The browser sends the URL to the domain name server (DNS), which searches for that URL in its database.
3. If the URL is found, the DNS sends the IP of that website to the web browser.
4. Using that IP the browser requests the web server of that website to send the specified web page to the web browser (done by HTTP/HTTPS).
5. Once the webpage is recieved, the browser renders the webpage and displays it to the user.
6. If the URL isn't in the DNS database, the DNS sends the URL to another DNS which also checks, if the URL isn't present in any of the DNS databases, the URL doesn't exist and the user is notified.

If the HTTPS protocol is being used, the web browser first asks for a digital certificate from the web server and sees if it is authentic, if not the user is informed that the webpage is not secure.

5.1.6 Cookies

Cookies are files that store data on the user's device. They can store data that is regularly used and hence save the user the boredom of inputting such things repeatedly (logins, usernames, etc). Cookies are used for the following:

- Saving personal details.
- Tracking user preferences.
- Holding items in an online shopping cart.
- Storing login details.

Cookies are of two types: session and permanent.

- Session: These are temporary cookies that only stay on your device as long as you are on a certain webpage, such as an online shopping cart which is on the device as long as you are shopping, but as soon as you close the webpage the data regarding your shopping cart is deleted from your device.
- Persistent: These cookies are permanent and remain on your device even after you close the webpage. Examples include the user's preferences on a certain webpage, etc.

5.2 Digital currency

5.2.1 Electronic existence

Currency that only exists electronically and is only exchanged amongst computers is called digital currency. Credit cards and mobile banking are examples.

5.2.2 Blockchains

Cryptocurrencies, such as Bitcoin and Dogecoin are decentralised currencies, i.e. no centralised authority is in charge of keeping track of the transactions made by these currencies. But the transactions must be kept track of nonetheless, this is done using blockchains.

A blockchain is a digital ledger, which is encrypted. That means whenever a transaction is made a new "entry" is added onto the blockchain, hence the transactions are recorded. Blockchains are irreversible meaning once an entry has been made no one can change it.

5.3 Cyber Security

5.3.1 Threats

When browsing the internet, there is a chance that data being transmitted across the network can be intercepted and stolen by potential hackers. They can do so in the following ways:

- Brute-force attack: Hackers will try to use possible combination of letters to maybe stumble upon your username and subsequently your password for a certain account of yours.

- Data interception: This is done by use of software known as packet sniffers, installed onto routers which can determine whether a packet passing through the router is useful, if it is then a copy of the packets are sent to the hacker.
- Distributed denial of service (DDoS): Malware (malicious software) is sent to many user's devices, all the devices being part of a network. This malware then sends requests to a certan web server, and since a server can only handle a certain number of requests, it literally gets overwhelmed and slows down to a snail's pace where it cannot handle any requests quick enough.
- Hacking: Hackers may exploit vulnerabilities in a network, to gain access to data being transmitted across the network; they brute-force attack a user's account, already discussed.
- Malware: Can be of various types:
  - Virus: Malware that replicates itself and corrupts, and slows down victim's computer by using up all available memory.
  - Worm: Similar to virus, only it clogs up the bandwidth of the network it is connected to.
  - Spyware: Malware that runs in the background as the unaware user uses his/her device and the spyware spies on the user, often stealing usernames and passwords and hence access to accounts and sends it on to the perpetrator. This can be done by means of a keylogger which simply records any and all keypresses by the user.
  - Trojan horse: Software that is meant to look exactly like another piece of software, once executed, releases other forms of malware onto the device.
  - Adware: Malware that automatically pops up advertisements, which is an irritating experience.
  - Ransomware: Encrypts user's data and asks for money in exchange for decryption of that data.
- Pharming: Used to obtain user's personal data. Once malware is installed, the user is sent to websites that look very much like the websites the user is going to but is actually set up by the perpetrator. The user then unknowingly enters their credentials, which are now known by the perpetrator.
- Phishing: The objective is same as pharming, only the perpetrator tricks the user to click a link, and the rest is same as pharming.
- Social engineering: Scammers, who trick users by lying, acting and decieving them.

5.3.2 Solutions

To save oneself from these threats we can use the following measures:

- Access levels: Only allow certain data to be accessible by users with administrator or higher levels.
- Anti-malware: Software that detects and reports malicious activity by software.
- Authentication: Setting very strong passwords, that are very difficult to guess, including unique characters such as numbers, varying cases in letters, etc. Biometrics can be used to make sure data can only be accessed by only the user with specific biological signatures such as fingerprints and retina scans. Lastly two-step verification can be used to make sure that even if perpetrators gain access to username and password, they require something that only you have to log into your account.
- Software updates: Outdated software may have vulnerabilities which hackers can exploit, to avoid this, one can automate the updating of software.
- Spelling and tone: To avoid being phished or pharmed, check email tone and spelling properly.
- Check attached URL: A link may say "to know more" but the URL behind attached may be something else. Check them to be safe.
- Firewalls: Software that examines incoming and outgoing data across a network. This can detect malicious transfers of data and report and block those transmissions.
- Proxy servers: Can be used by web servers to examine requests sent before they are sent to the actual server. As a result web servers are protected from DDoS attacks.
- Secure Sockets Layer (SSL): HTTPS uses the SSL protocol.

6 Automated and emerging technologies

6.1 Automated systems

6.1.1 Sensors, microprocessors and actuators

Inputs can be taken by sensors, processed (compared with stored values) by microprocessors and actions can be taken by actuators.

6.1.2 Automation in context

To consider the advantages and disadvantages of automated systems in given contexts, one can consider the following factors:

- Initial cost: Can be high to develop and install the system.
- Running cost: Will be low as employees need not be paid.
- Safety: Will be high as people need not work in dangerous places, people aren't working and so accidents are unlikely.
- Replacing people's jobs: Jobs automated by the system will be lost but more will be made in maintaining and operating the system.
- Continuous work: If the context requires 24/7 operation, it is an advantage.
- Precision: Of course automated devices are more precise.

6.2 Robotics

6.2.1 Characteristics of a robot

A robot consists of a physical, mechanical framework. Sensors, microprocessors and actuators and lastly they are programmable meaning they can be told to follow instructions.

6.2.2 Robotics in context

Identical to Automation in context.

6.3 Artificial intelligence (AI)

6.3.1 What is it?

It is a branch of computer science dealing with the simulation of intelligent behaviours by computers.

6.3.2 Characteristics for AI

Data must be collected and given to the AI so that it can reason, it must programmed with rules so that it can reason, the ability to reason and lastly the ability to learn from inputs given by users and hence adapt.

6.3.3 Machine learning and expert systems

Machine learning is when a system learns about information either by itself (unsupervised) or is told about information (supervised). A machine is given a picture of a horse and is told it is a picture of a horse, this is supervised, unsupervised may involve graph plotting.

Expert systems consist of a knowledge base which is a list of facts; a rule base which are facts that link the facts, an inference engine which decides what to ask next and when to ask it and lastly the user interface so that the user can communicate with the system.