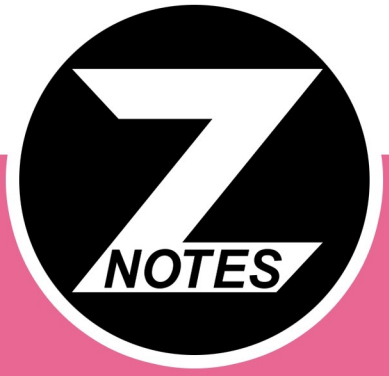
ZNOTES // IGCSE SERIES

visit www.znotes.org



Updated to 2017-19 Syllabus

CIE IGCSE COMPUTER SCIENCE 0478

SUMMARIZED NOTES ON THE THEORY SECTION

TABLE OF CONTENTS

1. Data Representation

1.1 Binary Systems

- The binary system is based on the number 2
- Made up of 1s and 0s
- Use of binary numbers in computer systems

Converting Binary to Denary

- To calculate a binary number like, 10101000, place it in columns of base 2 numbers
- Then add all the base 2 numbers

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

$128 + 32 + 8 = \mathbf{168}$

Converting Denary to Binary

- To calculate a denary number like, 84, set up the columns of base 2 numbers

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

01010100

1.2 Measurement of the Size of Computer Memories

- A binary digit is referred to as a **BIT**, 8 bits is a **byte**
- Byte is used to measure memory size

NAME OF MEMORY SIZE	NO. OF BITS	EQUIVALENT DENARY VALUE
1 kilobyte (1KB)	2^{10}	1 024 bytes
2 megabyte (1MB)	2^{20}	1 048 576 bytes
1 gigabyte (1GB)	2^{30}	1 073 741 824 bytes
1 terabyte (1TB)	2^{40}	1 099 511 627 776 bytes
1 petabyte (1PB)	2^{50}	1 125 899 906 842 624 bytes

Example use of binary

- A **register** is a group of bits, often depicted as:
  - **10010111**
- Robotics
- Digital instruments
- Counting systems

1.3 Hexadecimal

- Closely related to the binary system
- Hexadecimal is a base 16 system
- Numbers 0 to 9 and letters A to Fare used to represent each hexadecimal digit
- A =10, B = 11, C = 12, D = 13, E = 14, F = 15

HEXADECIMAL VALUE	DENARY VALUE
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
A	10
B	11
C	12
D	13
E	14
F	15

Converting Binary to Hexadecimal

- To convert binary number 01100001
  - Separate into two nibbles (4 bits)
  - Convert nibbles to denary
  - Change denary numbers to hex if needed (e.g. 10 = A)

8	4	2	1		8	4	2	1
0	1	1	0		0	0	0	1

$= 6$ $= 1$

hex value **61**

Converting Hexadecimal to Binary

- To convert hex value 6C
  - Change hex value to denary numbers (e.g. 12 = C)
  - Separate hex value and convert to 4 bit binary value
  - Put the two nibbles together to form an 8 bit binary

hex value 6 to binary *hex value C (12) to binary*

8	4	2	1		8	4	2	1
0	1	1	0		1	1	0	0

01101100

Converting Denary to Hexadecimal

- To convert denary number 98
  - Convert to binary
  - Split the binary (8bits) into nibbles (4bits)
  - Find the values separately

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

$= \mathbf{6}$ $= \mathbf{2}$

Converting Hexadecimal to Denary

- To convert hex value 2B
  - Split the hex value into two
  - Convert each number to binary
  - Put the two binary numbers together
  - Convert to denary

hex value 2 to binary *hex value B (11) to binary*

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

$= \mathbf{43}$

1.4 Use of the Hexadecimal System

- **Examples:**
  - defining colours in Hypertext Markup Language (HTML)
  - Media Access Control (MAC) addresses
  - Assembly languages and machine code
  - Debugging

Memory Dumps

- Hexadecimal is used when developing new software or when trying to trace errors
- Memory dump is when the memory contents are output to a printer, monitor.

Assembly code and machine code (low level languages)

- Computer memory is machine code/ assembly code
- Using hexadecimal makes it easier, faster, less error prone to write code compared to binary.
- Using machine code (binary) takes a long time to key in values and prone to errors

1.5 Error Checking

Parity Checking

- Parity checking is used to check weather data has been changed or corrupted following transmission from one device to another
- A byte of data is allocated a parity bit
  - Systems that use even parity have an even number of 1-bits
  - Systems that use odd parity have an even number of 1-bits

Automatic Repeat Request (ARQ)

- ARQ is another method to check if data has been transmitted correctly
- It uses and acknowledgement (message sent by the receiver indicating that data has been received correctly)

Checksum

- Checksum is another way to see if data has been transmitted correctly
- Data is sent in blocks and an additional value sent at the end of the block

Echo check

- When data is sent to another device, this data is sent back again to the sender
- The sender compares the two sets to check if any errors occurred
- Not reliable

1.6 File types

Musical Instrument Digital Format (MIDI)

- Storage of music files
- Communications protocol that allows electronic musical instruments to interact with each other
- Stored as a series of demands but no actual music notes
- Uses 8-bit serial transmission (asynchronous)
- Each MIDI command has a sequence of bytes:
  - First byte is the status byte – informs the MIDI device what function to preform
  - Encoded in the status byte is the MIDI channel (operates on 16 different channels)
- Examples of MIDI commands:
  - Note on/off: indicates that a key has been pressed
  - Key pressure: indicates how hard it has been pressed (loudness of music)
- Needs a lot of memory storage

MP3

- Uses technology known as Audio Compression to convert music and other sounds into an MP3 file format
- This compression reduces the normal file size by 90%
  - Done using file compression algorithms which use Perceptual Music Shaping
  - Removes sounds that human ear cannot hear properly
  - Certain sounds are removed without affecting the quality too much

- CD files are converted using File Compression Software
- Use lossy format as the original file is lost following the compression algorithm

MP4

- This format allows the storage of multimedia files rather than just sound
- Music, videos, photos and animations can be stored
- Videos, could be streamed without losing any real discernible quality

Joint Photographic Experts Group (JPEG)

- JPEG is a file formats used to reduce photographic file sizes
- Reducing picture resolution is changing the number of pixels per centimetre
- When photographic file undergoes compression, file size is reduced
- JPEG will reduce the raw bitmap image by a factor between 5 and 15

1.7 Lossless and Lossy File Compression

Lossless File Compression

- All the data bits from the original file are reconstructed when the file again is uncompressed
- Important for files where loss of data would be disastrous (spreadsheet)

Lossy File Compression

- The file compression algorithm eliminates unnecessary bits of data like MP3 and JPEG formats
- Impossible to get original file back once compressed

2. COMMUNICATION & INTERNET TECHNOLOGIES

2.1 Transmission of Data

- *Asynchronous data transmission* refers to data being transmitted in an agreed bit pattern
  - Data bits are grouped together & sent with control bits
  - This means the receiver of the data knows when the data starts and ends, prevents data getting mixed up
- *Synchronous data transmission* is a continuous stream of data (not in discrete groups like asynchronous)
  - Ensures that the sender and receiver are synchronised with each other
  - Faster method

2.2 Serial & Parallel Transmission

- *Serial data transmission* is when data is sent one bit at a time over a single wire
  - Works well over long distances
  - Data transmitted at a slower rate (USB)
- *Parallel data transmission* is when data several bits (1 byte) are sent down several wires at the same time
  - Works well over short distance
  - Faster method (internal components use parallel for high speed)

2.3 Simplex, Half-duplex and Full-duplex

- *Simplex data transmission* is in one direction only (e.g. computer to printer)
- *Half-duplex data transmission* is in both directions but not at the same time (e.g. phone conversation where only one person speaks)
- *Full-duplex data transmission* is in both directions simultaneously (e.g. broadband connection on phone line)

2.4 Universal Serial Bus (USB)

- USB is an asynchronous serial data transmission method
- USB consists of:
  - Four-wire shielded cable
  - Two wires used for power and earth
  - Two wires used in data transmission

ADVANTAGES	DISADVANTAGES
Automatically detected	
Only fit one way, prevents incorrect connections	Maximum cable length is about 5 metres
Different data transmission rates	Transmission rate is less than 500 mb/sec

2.5 Security Aspects

Hacking

- The act of gaining illegal access to a computer system
- Effect:
  - Leads to identity theft, gaining personal information
  - Data can be deleted, changed or corrupted
- To remove risk:
  - Firewalls
  - Strong passwords/ user IDs
  - Use of anti-hacking software

- Difference between hacking and cracking
  - Hacking breaks into computer system to steal data
  - Cracking is where someone edits a program code, malicious

Viruses:

- Program that can replicate itself with the intention of deleting or corrupting files, cause computer malfunction
- Effect:
  - Can cause computer to crash
  - Can delete or corrupt files/data
- To remove risk:
  - Install anti-virus software
  - Don't use software from unknown sources
  - Be careful when opening emails from unknown

Wardriving:

- The act of locating and using wireless internet connections illegally
- Effects:
  - Possible to steal internet time
  - Possible to hack into wireless network and steal user's password
- To remove risk:
  - Use complex passwords
  - Firewalls

Spyware:

- Software that gathers info by monitoring key presses on the user's keyboard and info is sent back
- Effects:
  - Access to all data entered
  - Software is able to install other spyware, read cookie data
- To remove risk:
  - Use of anti-spyware software
  - Use a mouse to select characters from passwords rather than typing them

2.6 Internet Principles of Operation

- **Internet Service Protocol:** These are companies that provide user with access to the internet

Internet Protocol (IP) Address

- Each device on the internet is given a unique address known as the IP address
- 32-bit number written in the form: 109.108.158.1
- IP address gives the location of a device on the internet whereas the MAC address identifies the device connected to the internet
- IP address changes, MAC address remains unchanged

HTML (HyperText Mark-up Language)

- Used when writing and developing pages
- Mark-up language is used in the processing
- Html use <tags> to bracket piece of codes
- Different intensity of colours is determined by its hexadecimal value

Media Access Control (MAC)

- MAC address refers to a number which uniquely identifies a device on the internet
- Refers to the network interface card (NIC) which is part of the device
- Usually made up of 48 bits shown as six groups of hexadecimal digits
- NN:NN:NN:DD:DD:DD
  - (NN:NN:NN) first half is the identity number of the manufacturer of the device
  - (DD:DD:DD) second half is the serial number of the device
- Types of MAC Address:
  - Universally Administrated MAC Address (UAA)
  - Locally Administrated MAC Address (LAA)
  - UAA is the most common type set by the manufacturer
- Reasons to change MAC address using LAA
  - To ensure they follow the correct formula
  - To bypass MAC address filter on a router or a firewall
  - To get past certain types of network restrictions

Web addresses

- Each character on the keyboard has its own ASCII code
- Can be represented using hexadecimal or decimal values
- Hexadecimal addresses are used in the address of files or webpages as a security figure
- Takes longer to type in URL but advantage is that you are unlikely to fall into the trap of copying a fake website

Cookies

- A packet of information sent by a web server to a web browser
- Generated each time the user visits the website

- Every time a user visits a website, cookies will have collected some key information about the user
- They are able to carry out user tracking and maintain user preferences
- Cookies are pieces of data
- Information gathered by cookies doesn't contain personal information

3. Hardware & Software

3.1 Logic Gates

- **Logic Gates:** use one or more inputs and produces a single logical output
- **AND gate:** If both inputs high, output is high

$A.B$

A	B	Output
0	0	0
0	1	0
1	0	0
1	1	1

- **OR gate:** If either inputs high, output is high

$A + B$

A	B	Output
0	0	0
0	1	1
1	0	1
1	1	1

- **NOT gate:** an inverter

$\bar{A}$

A	Output
1	0
0	1

- **NAND gate:**

$\overline{A.B}$

A	B	Output
0	0	1
0	1	1
1	0	1
1	1	0

- **NOR gate:**

$\overline{A + B}$

A	B	Output
0	0	1
0	1	0
1	0	0
1	1	0

- **XOR gate:**

$\overline{A \oplus B}$

A	B	Output
0	0	0
0	1	1
1	0	1
1	1	0

3.2 Computer Architecture & Fetch-Execute Cycle

Computer Architecture

- *Address bus* – unidirectional
- *Data bus* – bi-directional
- *Control bus* – unidirectional and bi-directional

- **Processor:** The processor contains the Arithmetic and Logic Unit (ALU)
- **Control Unit:** The control unit controls the operation of the memory, processor and input/output devices

The Fetch-Execute Cycle

1. PC contains address of the next instruction to be fetched
2. This address is copied to the MAR via the address bus
3. The instruction of the address is copied into the MDR temporarily
4. The instruction in the MDR is then placed in the CIR
5. The value in the PC is incremented by 1, pointing the next instruction to be fetched
6. The instruction is finally decoded and then executed

3.3 Input Devices

SCANNERS:

Two-dimensional Scanners:

- Used to input hard-copy documents
- The image is converted into an electronic form which can be stored in the computer
  - Document is placed on a glass panel
  - A bright light illuminates the document
  - A scan head moves across the document until the whole page is scanned. And image of the document is produced and sent to a lens using a series of mirrors
  - The lens focuses the document image
  - The focused image now falls onto a *charge couple device (CCD)* which consists of a numbers of integrated circuits
  - Software produces a digital image from the electronic form

- *Optical Character Recognition (OCR)* is a software which converts scanned documents into a text file format
- If the original document was a photo/image, then the scanned image forms an image file such as JPEG

Three-dimensional Scanners

- 3D scanners can scan solid objects and produce a three-dimensional image
- Scanners take images at several points, x, y and z (lasers, magnetic, white light)
- The scanned images can be used in *Computer Aided Design (CAD)* or to a 3D printer to produce a working model

Application of 2D Scanners at an Airport:

- Make use of (OCR) to produce digital images which represent the passport pages
- Text can be stored in ASCII format
- The 2D photograph in the passport is also scanned and stored as jpeg image
- The passenger's face is also photographed using a digital camera and compared using face recognition software
- Key parts of the face are compared (distance between eyes, width of nose)

Barcode readers/scanners

- A barcode is a series of dark and light parallel lines of varying thicknesses
- The numbers 0 -9 are each represented by a unique series of lines
- The left and right hand sides of the barcode are separate using guard bars
- Allows barcode to be scanned in any direction
  - Barcode is read by a red laser or red LED
  - Light is reflected back off the barcode; dark areas reflect little light which allows the bars to be read
  - Reflected light is read by sensors (photoelectric cells)
  - Pattern is generated which is converted to digital

Quick Response (QR) Codes

- Another type of barcode is the QR codes
- Made up of a matrix of filled in dark squares on a light background
- Can hold more storage (7000 digits)
- Advantages of QR codes:
  - No need for the user to write down website address
  - QR codes can store website addresses

Digital Cameras

- Controlled by microprocessor which automatically adjusts the shutter speed, focus the image, etc.
- Photo is captured when light passes through the lens onto a light sensitive cell
- Cell is made up of pixels
- Number of pixels determines size of the file

Keyboards

- Connected to computer with a USB connection or by wireless connection
- Each character has an ASCII value and is converted into a digital signal
- Slow method
- Prone to errors

Pointing devices

- Mouse/trackball
  - Traditional; mechanical ball, connected by USB port
- Modern type; red LEDs to detect movement

Microphones

- Used to input sound to a computer
- When a microphone picks up sound, a diaphragm vibrates producing an electric signal
- The signal goes to a sound card and is converted into digital values and stored in computer
- *Voice recognition,* voice is detected and converted into digital

Touchscreens

- Capacitive (medium cost tech)
  - Made up of many layers of glass
  - Creating electric fields between glass plates in layers
  - When top layer of glass is touched, electric current changes
  - Co-ordinates where the screen was touched is determined by an on-board microprocessor
- Infra-red *heat* (expensive)
  - Use glass as the screen material
  - Needs warm object to carry an input operation
- Infra-red *optical* (expensive)
  - Uses glass as screen material
  - Uses an array of sensors (grid form)
  - Point of contact is based on which grid co-ordinate is touched

- Resistive (inexpensive)
  - Upper layer of polyester, bottom layer of glass
  - When the top polyester is touched, the top layer and bottom layer complete a circuit
  - Signals are then sent out which are interpreted by a microprocessor, determine where screen was touched

Sensors

- Devices which read or measure physical properties
- Data needs to be converted to digital
- *Analogue to Digital Converter (ADC)* converts physical values into digital

Control of Street Lighting

- Light sensor sends data to the ADC
- Digitises data and sent to the microprocessor
- Microprocessor samples data every minute
- If data from sensor < value stored in memory:
  - Signal sent from microprocessor to street lamp
  - Lamp switched on

3.4 Output Devices

PRINTERS:

Inkjet Printers

- Used to print one-off pictures and documents

1. Data from document sent to printer driver
2. Printer driver ensures data is in correct format
3. Check made by printer driver that chosen printer is available
4. Data is sent to printer, stored in a temporary memory (printer buffer)
5. Sheet of paper is fed; sensor detects if paper is available in paper tray
6. Print head moves across paper printing text/image, four ink colours sprayed in exact amount
7. Paper is advanced so next line is printed
8. Repeated until buffer is empty
9. Once it is done, printer send an interrupt to the processor (request for more data to be sent)

Laser Printers

- Used to print flyers, high quality
- Use dry powder ink (toner) and static electricity to produce text and images
- Prints the whole page in one go

1. (steps 1-4 same as inkjet)
2. Printing drum is given a positive charge; as the drum rotates, a laser beam is scanned across it removing the positive charge leaves negatively charged areas which match the text/image
3. Drum is then coated with positively charged *toner*, it only sticks to negatively charged parts of the drum
4. A negatively charged sheet is rolled over the drum
5. Toner on the drum now sticks to the paper to produce copy of page
6. Paper finally goes through a fuser (set of heated rollers); heat melts the ink so it is permanent
7. Discharge lamp removes all electric charge from the drum, ready to print next page

3D Printers

- Used for models of cars
- Produce solid objects that work
- Built up layer by layer, using powdered resin, ceramic powder
- A design is made using Computer-aided Design (CAD)

2D and 3D Cutters

- 3D cutters can recognise objects in x, y, z direction
- 3D laser cutters can cut; glass, crystal, metal, wood

Actuators

- Used in many control applications involving sensors and devices (ADC and DAC)

Loudspeakers/Headphones

- Sound is produced by passing the digital data through a DAC then through amplifier and then emerges from loudspeaker
- Produced by voltage differences vibrating a cone in the speaker at different frequencies

LCD and LED Monitors

- Front layer of monitor is made up of *Liquid Crystal Display* (LCD), these tiny diodes are grouped together in threes as pixels (LCD doesn't emit any light)
- LCD monitors are back lit using *Light Emitting Diode (LED)* because:
  - LEDs reach their maximum brightness immediately
  - LEDs sharpens image (higher resolution), CCFL has yellow tint
  - LEDs improve colour image

- Monitors using LED are much thinner than CCFL
- LEDs consume very little power

- Before LEDs, LCD monitors were backlit using CCFL
- CCFL uses two fluorescent tubes behind the LCD screen which supplies the light source

LIGHT PROJECTORS:

- Two common types of light projectors:
  - Digital Light Projector (DLP)
  - LCD Projector
- Projectors are used to project computer output onto larger screens/interactive whiteboards

Digital Light Projectors (DLP)

- Uses millions of micro mirrors
- the number of micro mirrors and the way they are arranged on the DLP chip determines the resolution of the image
- When the micro mirrors tilt towards the light source they are *on*
- When the micro mirrors tilt away from the light source they are *off*
- This creates a light or dark pixel on the projection screen
- A bright white light source passes through a colour filter on its way to the DLP chip
- White light splits into primary colours

LCD Projectors

- Older technology than DLP
- A powerful beam of white light is generated from a bulb
- This beam of light is then sent to a group of chromatic-coated mirrors; these reflect the light back at different wavelengths
- When the white light hits the mirrors, the reflected light has wavelengths corresponding to red, green and blue
- These three different light pass through three LCD screens; these screens show the image to be projected as millions of pixels in grayscale
- When the coloured light passes through the LCD screens, a red, green and blue version of the grey image emerges
- Finally, the image passes through the projector lens onto the screen

3.5 Memory, Storage Devices & Media

PRIMARY MEMORY:

Random Access Memory (RAM)

- Features of RAM
  - Volatile/temporary memory (contents lost if RAM is turned off)
  - Used to store; data, files
  - It can be written to or read from and the contents from the memory can be changed
- Larger the size of the RAM, faster the computer will operate
- RAM never runs out of memory, continues to run slow
- As RAM becomes full, the processor has to continually access the hard drive to overwrite old data on RAM with new data

Read Only Memory (ROM)

- Features of ROM
  - Non-volatile/permanent memories (contents remain even when ROM is turned off)
  - Used to store start up instruction (basic input/output systems)
  - Data/contents of a ROM chip can only be read, cannot be changed

SECONDARY STORAGE:

Hard Disk Drives (HDD)

- Data is stored in a digital format on the magnetic surface of the disks (platter)
- Number of read/write heads can access all of the surfaces of the disk
- Each platter will have two surfaces which can be used to store the data
- Data is stored on the surfaces in sectors and tracks
- HDD have very slow data access compared to RAM

Solid-State Storage (SDD)

- No moving parts and all data is received at the same time (not like HDD)
- Store data by controlling the movement of electrons within NAND chips, as 1s and 0s
- Non-volatile rewritable memory
- Benefits of using SDD rather than HDD:
  - More reliable (no moving parts)
  - Considerably lighter (suitable for laptops)
  - Lower power consumption

- Run much cooler than HDDs
- Very thin
- Data access if faster than HDD

- Drawback – questionable longevity (20GB per day)

OFF-LINE STORAGE

CD/DVD Disks

- Laser (red) light is used to read and write data in the surface of the disk
- Use a thin layer of metal alloy to store data
- Both systems use a single, spiral track which runs from the centre of the disk to the edge
- DVD uses *Dual-Layering* which increases the storage capacity (two individual recoding layers)

Blu-ray Disks

- Uses blue laser to carry out read and write operations
- Wavelength of laser light is less than CD and DVD (stores up to five times more data than DVD)
- Automatically come with secure encryption (prevent piracy and copyright infringement)
- Used as back-up systems

USB Flash Memories

- Very small, lightweight suitable from transferring files
- Small back-up devices for photo, music
- Solid state so need to be treated with care

3.6 High- & Low-Level Languages

High-Level Languages

- Easier to read and understand as the language is closer to human language
- Easier to write in shorter time
- Easier to debug at the development stage
- Easier to maintain once in use

Low-Level Languages

- Refer to machine code
- Binary instructions that computer understands

TRANSLATORS:

- A program must be translated into binary before a computer can use it
- Types of translators; Compiler, Interpreter and Assembler

Compiler

- Translates a program written in high-level language into machine code
- Used without compiler
- Executable file of machine code produced
- One high-level language translated into several machine code instructions
- Used for general use

Interpreter

- Executes a high-language program a statement at a time
- No executable file of machine code produced
- One high-level language program statement may require several machine code instructions to be executed
- Cannot be used without interpreter
- Used when program is being developed

Assembler

- Translates a low-level language program into machine code
- Executable file of machine code produced
- One low-level language translated into one machine code instructions
- Can be used without assembler
- Used for general use

Syntax Errors:

- When program is being compiled, if any syntax errors are found no translated program is produced
- Instead, a list of all errors in program is produced
- Programmer corrects program and recompiles
- When a program is being interpreted, the interpreter preforms the action until syntax error is found
- The programmer is the alerted to the place in the program where error was found
- The error is corrected and interpretation continues

4. SECURITY

- Need to keep data safe from accidental damage, including corruption and human errors
- Need to keep data safe from malicious actions, including unauthorised viewing, deleting, copying and corruption

4.1 Firewalls & Proxy Servers

- A *firewall* sits between the user's computer and an external network (internet) and filter information in and out of the computer
- Tasks carried out by firewall:
  - Examining 'traffic'
  - Checking weather incoming or outgoing data meets criteria
  - If data fails the criteria, the firewall blocks 'traffic'
  - Firewall can keep a list of all undesirable IP addresses
  - Helping to prevent viruses or hackers entering the user's computer
- *Proxy servers* act as an intermediary between the user and a web server
- Functions of proxy servers:
  - Allowing the internet 'traffic' to be filtered
  - By using *cache,* they can speed up access to information from a website
  - Keeping the user's IP address secret
- Acting as a firewall

4.2 Security Protocols

Secure Sockets Layer (SSL)

- Type of protocol that allows data to be sent and received securely over the internet
- When a user logs onto a website, SSL encrypts the data
- https or padlock in the status bar
- When user wants to access a secure website:
  - User's web browser sends a message so it can connect with required website which is secured by SSL
  - Web browser requests that the web server identifies itself
  - Web server responds by sending a copy of its SSL certificate
  - Web browser checks if certificate is authentic
  - Sends signal back to web browser
  - Starts to transmit data once connection is established
  - If not secure, browser will display an open padlock

Transport Layer Security (TLS)

- Form of protocol that ensures the security and privacy of data between devices and users when communicating over the internet
- Designed to provide encryption, authentication and data integrity in a more effective way than SSL
- Possible to extend TLS by adding new authentication methods

4.3 Encryption

- Used to protect data in case it has been hacked
- Doesn't prevent hacking, makes data meaningless

Symmetric Encryption

- A secret key which can be a combination of characters
- If this key is applied to a message, its contents is changed
- One key is needed to encrypt a message and another key is needed to decrypt a message
- Increasing the length of the key increases the strength of the encryption

Plain text and Cypher Text

- Plain text is the normal representation of data before it goes through an encryption algorithm
- Cypher text is the output from an encryption algorithm

Authentication

- Authentication is used to verify that data come from a trusted source
- Works with encryption to strengthen internet security
- Passwords: usually a user id/name and password are used to log on to systems
- Digital Signatures: public key encryption; ensure an electronic document is authentic
- Biometrics: relies on the unique characteristics of human beings (fingerprint scans, retina scans)

4.4 Phishing, Pharming & DoS

Phishing:

- Creator sends out a legitimate-looking email; as soon as recipient clicks on link, user is sent to a fake website
- Effect:
  - Creator of email can gain personal data; bank account
  - Can lead to fraud
- To remove risk:
  - Many ISPs filter out phishing emails
  - User should be cautious

Pharming

- Malicious code installed on a user's hard drive or on the web server, code will redirect the user to a fake website
- Effect:
  - Creator of malicious code can gain personal data; bank account
  - Can lead to fraud or identity theft

- To remove risk:
  - Some anti-spyware can identify and remove pharming code from hard drive
  - User should be alert

Denial of Service Attacks (DoS)

- An attempt at preventing users from accessing part of a network
- Usually temporary but may be damaging
- Attacker me be able to prevent user from:
  - Accessing their emails
  - Accessing websites
  - Accessing online services

4.5 Applications

- Ways bank protect their costumers from online fraud
  - Banks use 10/12-digit code unique to the costumer
  - May be asked to input three random numbers from a four-digit PIN
  - Some use a hand-held device into which a customer inserts their card. Device will generate an eight-digit code which the customer types into web page
  - Some ask to key in parts of their passwords using drop-down boxes (using a mouse)

5. ETHICS

- A set of principles set out to regulate the use of computers
- *Plagiarism* is when a person takes another person's idea/work and claims it as their own

5.1 Types of Softwares

Free Software

- Software source code can be freely accessed and modified as required
- Run, copy, change or adapt free software (e.g. Scribus, Abiword)
- Possible to distribute modified versions of software to friends and family

Freeware

- A software a user can download from the internet free of charge
- Once it has been downloaded, there are no fees associated (e.g. Adobe, Skype)
- Subject to all copyright laws
- User is not allowed to study, modify code

Shareware

- All the features of the full version of software are not made available; full version needs to be purchased first
- Subject to all copyright laws
- Permission needs to be obtained before software is copied and given to friends or family

CIE IGCSE COMPUTER SCIENCE//0478