H2 Computing Year 1 + 2 Theory Summary

This document contains the notes removed due to the removal of Common Last Topics for the 2021 A Levels

ENCRYPTION: Process of **encoding** a message in such a way that **only authorized parties can access it**

Sender: uses a secret key and encryption algo to encrypt plaintext into a cipher.

Receiver: uses a secret key and decrypt algo to descript cipher back to og plaintext.

SYMMETRIC ENCRYPTION: Same single encryption and decryption key that is shared between sender and receiver.

+: Fast processing

-: Low security if the key is intercepted

Standard: AES (Advanced Encryption Standard)

ASSYMETRIC ENCRYPTION: One **public** key and one **private** key that are mathematically related. One cannot be derived from another. | RSA (Rivest-Sharmir-Adleman)

Sender uses receiver's public key to encrypt message. The receiver's private key is the only key that decrypts msg.

+: Even with public key, message not leaked ; More secure

-: Slower than symmetric encryption

DIGITAL SIGNATURE (DS): Encryption and Decryption technology that **secures data associated** a signed document and **verifies the authenticity** of the document.

Authentication: Ensures message from known sender

Non-repudiation: Sender cannot deny that they sent it

Integrity: Message is not altered in transit

Usage: Used on emails, internet, bloc chains.

Technologies: Hashing ; Encryption (Priv + Public Keys)

Hashing: Generates a short unique text string, acts as a unique digital fingerprint. | SHA256 (Secure Hash Algo)

~ (SENDER): The sender uses a hash algo to create hash. Private key encrypts hash to DS. Msg & DS sent to receiver.

~ (RECEIVER): The receiver uses the sender's public key to decrypt the DS back to the sender's hash.

IDENTIFICATION: user claims an identity.

AUTHENTICATION: Users proving their identity by providing credentials. System validates the identity of the user. E.g: Password, Fingerprint, Retina, Secret Qns, OTP

HASHING: Sender public key to decrypt the digital signature back to the sender's version of hash. Receiver uses the same hash algo to create new hash from msg. If hashes match, the data is not altered.

AUTHORISATION: System validates the granted the permission of an authenticated user to access resources.

DATA VALIDATION: Chk data format valid; Length checks

DATA VERIFICATION: Check that data is what user intends to give. E.g double input of password.

MALWARE: Malicious software that is harmful to the computer system. Can alter/disable/destroy/steal data from computer, mobile devices and the network.

Virus: Attaches itself to a file/program ; Remains dormant until executed ; Replicate to infect other computers

Worm: No need to be attached to files ; Self-replicating.

Trojan Horse: Appears as legit program ; Once it gains the access into the computer, it runs malicious code that damages the computer. Does NOT replicate itself.

Ransomware: Locks computer, encrypts the data ; Forces the user to pay a ransom to get data back.

DENIAL OF SERVICE (DOS): Attacks network traffic to exhaust resources, cannot fulfil legitimate requests.

DDOS (DISTRIBUTED DOS): Multiple compromised devices (using botnets) to attack systems.

SOCIAL ENGINEERING ATTACK: Use of deception and trickery to convince users to compromise their systems.
Phishing: attacker sends email address that impersonates a company, asking for bank account details

Spoofing: attacker conceals identity, IP/MAC address

Spam: users flooded w messages full of ads and viruses.

PROTECTION SCHEME: Update OS, install antivirus, do not click suspicious links, do not connect to public WiFi

Firewall: **monitor and control** all in/outcoming NW traffic, but hackers can bypass and does not block internal attacks

Proxy Server: Acts as intermediary for req from clients, hides IP address and details, control in/out NW traffic

VPN: Adds encryption on any data transmitted in and out

IDS: Scans, monitor NW traffic, sounds alert but no action.

Signature Based: Pre-defined set of rules to identify traffic.
Limitation: cannot detect unknown attacks.

Anomaly Based: Database of unacceptable traffic patterns.
Limitation: inaccurate profile, difficult to determine cause.

IPS: IDS, but **blocks** unauthorised access. May drop packets, reset connections, sound alerts.