

Topic 6: Security, Privacy and Data Integrity

Keyword sheet - Cambridge AS & A Level Computer Science 9618. Tick each term once you can define it from memory.

Keyword	Definition	Know it?
Security / privacy / integrity	Protection from unauthorised access / control over personal data / accuracy and consistency of data.	
Authentication	Verifying a user's identity, e.g. password, biometrics, two-step verification.	
Firewall	Filters network traffic against rules to block unauthorised access.	
Proxy server	Intermediary that filters requests, caches content and hides internal addresses.	
Anti-malware	Software that detects, quarantines and removes malicious code.	
Virus / worm / Trojan horse	Attaches to files and replicates when run / self-replicates over networks / disguised as legitimate software.	
Spyware / ransomware	Secretly gathers information / encrypts files and demands payment.	
Phishing / pharming	Fraudulent messages seeking credentials / redirection to a fake site through DNS or host file manipulation.	
DDoS / brute-force	Overwhelming a server with requests from many sources / trying all possible credentials.	
Encryption	Scrambling data with an algorithm and key so it is unreadable to unauthorised parties.	
Symmetric / asymmetric encryption	Same key for both operations / public key encrypts and private key decrypts.	
Digital signature	Hash of a message encrypted with the sender's private key, proving origin and integrity.	
Validation	Automated check that data is reasonable: range, length, type, presence, format, check digit.	
Verification	Check that data is copied or entered correctly: double entry, visual check, parity, checksum.	
Check digit	Digit calculated from other digits and appended to detect transcription errors.	
Parity check / checksum	Odd/even count of 1s / value calculated from a data block to detect transmission errors.	
Backup / archive	Copy of data kept to restore after loss / long-term storage of data not in regular use.	