

Topic 17: Security

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

Keyword	Definition	Know it?
Plaintext / ciphertext	Original readable data / encrypted data.	
Symmetric encryption	Single shared key; fast but the key distribution problem exists.	
Asymmetric encryption	Key pair: public key to encrypt, private key to decrypt; slower.	
Quantum cryptography	Uses photon polarisation (qubits) to exchange keys; eavesdropping alters the quantum state and is detected.	
SSL / TLS	Protocols that provide encrypted, authenticated communication; use a handshake to agree a session key.	
Session key	Temporary symmetric key used for one session.	
Digital certificate	Electronic document binding a public key to an identity, signed by a certificate authority.	
Certificate authority (CA)	Trusted third party that issues and verifies digital certificates.	
Digital signature	Encrypted hash of a message proving authenticity and integrity.	
Hash function	One-way function producing a fixed-length digest from data.	
Confidentiality / integrity / authenticity	Security aims: only authorised access / unchanged data / verified source.	
Man-in-the-middle attack	Attacker intercepts and may alter communication between two parties.	