Topic 17: Security

EAL keyword sheet - Cambridge International AS & A Level Computer Science 9618. Write the word in your own language in the last column.

Keyword	Meaning	Example sentence	In my language
encryption	Changing data into a code so it is unreadable without a key.	*Encryption protects emails.*	
plaintext / ciphertext	Data before encryption / data after encryption.	*Ciphertext looks like random characters.*	
symmetric encryption	The same key is used to encrypt and decrypt.	*Sharing the key safely is a problem.*	
asymmetric encryption	A public key encrypts, a private key decrypts.	*Anyone can use the public key.*	
public key	A key that can be shared with everyone.	*Send me your public key.*	
private key	A key that is kept secret.	*Only the owner has the private key.*	
key distribution problem	The difficulty of sharing a secret key safely.	*Asymmetric encryption solves key distribution.*	
quantum cryptography	Using quantum properties of light to share keys securely.	*Quantum cryptography can detect eavesdropping.*	
qubit	A quantum bit that can be in more than one state at once.	*A qubit is not only 0 or 1.*	
SSL / TLS	Protocols that create a secure encrypted connection.	*TLS protects data sent to a website.*	
handshake	The first messages two computers exchange to set up a secure connection.	*The TLS handshake agrees a session key.*	
session key	A temporary symmetric key used for one connection.	*The session key encrypts the data.*	
digital certificate	An electronic document that proves the owner of a public key.	*The website has a digital certificate.*	
certificate authority (CA)	A trusted organisation that issues digital certificates.	*The CA checks the website's identity.*	
digital signature	A way to prove who sent a message and that it has not been changed.	*A digital signature uses a hash.*	
hash function	A function that turns data into a fixed-length value.	*A hash cannot be reversed.*	

Keyword	Meaning	Example sentence	In my language
authenticity	Proof that something is real and from the claimed source.	*A certificate shows authenticity.*	
integrity	Data has not been changed.	*A hash checks integrity.*	
confidentiality	Only authorised people can see the data.	*Encryption gives confidentiality.*	
man-in-the-middle attack	An attacker secretly intercepts communication between two parties.	*HTTPS helps stop man-in-the-middle attacks.*	
eavesdropping	Secretly listening to or reading data in transit.	*Wi-Fi eavesdropping is possible without encryption.*	
trusted	Believed to be reliable.	*Browsers trust well-known CAs.*	