17. Security

Starter Quiz ·

A-Level Computer Science Name: _____ Score: _____

1. Symmetric encryption uses:
   - ☐ a public key and a private key
   - ☐ the same key to encrypt and decrypt
   - ☐ no key at all
   - ☐ a one-way hash

2. TLS provides which combination of protections for data in transit?
   - ☐ encryption, authentication and integrity
   - ☐ faster downloads only
   - ☐ spam filtering
   - ☐ compression only

3. What is the main job of QKD?
   - ☐ Remove the need for identity checks
   - ☐ Store the whole message in a certificate
   - ☐ Share key material

4. To send a confidential message to Alice using asymmetric encryption, you encrypt with:
   - ☐ Alice's public key (only her private key can decrypt it)
   - ☐ your own private key
   - ☐ a shared session key
   - ☐ Alice's private key

5. Which protections does TLS provide for data in transit? Select **all** that apply.
   - ☐ integrity, so tampering in transit is detected
   - ☐ a guarantee that the data will arrive
   - ☐ authentication of the server's identity
   - ☐ encryption, so an eavesdropper reads only ciphertext

   Tick every correct option.

6. An attacker can always copy an arbitrary unknown quantum state perfectly and leave it unchanged.

   ☐ True ☐ False

7. Bob wants Alice to be sure a message really came from him. Which key does Bob use to create the digital signature?
   - ☐ Alice's public key
   - ☐ Alice's private key
   - ☐ Bob's public key
   - ☐ Bob's private key

8. A digital signature proves authenticity and integrity (who signed it, and that nothing changed) but does NOT hide the message – you must encrypt it as well for confidentiality.

   ☐ True ☐ False

9. Six of 40 sample bits differ. What percentage differ?

   _____ %

10. A cryptographic hash produces a fixed-size _____ from an input of any size.

    _____

17. Security

Answers ·

A-Level Computer Science

1. **the same key to encrypt and decrypt**

   Symmetric encryption shares one secret key – fast, but it must be distributed securely.

2. **encryption, authentication and integrity**

   TLS encrypts the traffic, authenticates the server (via a certificate) and detects tampering (integrity).

3. **Share key material**

   QKD shares key material; an encryption scheme uses a key to protect the message.

4. **Alice's public key (only her private key can decrypt it)**

   Encrypting with the recipient's public key means only their matching private key can decrypt it.

5. **integrity, so tampering in transit is detected; authentication of the server's identity; encryption, so an eavesdropper reads only ciphertext**

   Delivery is TCP's job. TLS adds confidentiality, identity and tamper-detection on top of it.

6. **False**

   An unknown state cannot be perfectly cloned; interception can affect measured results.

7. **Bob's private key**

   Only Bob holds his private key, so only he can produce the signature; Alice checks it with Bob's public key. Confidentiality uses the receiver's keys, a signature uses the sender's.

8. **True**

   Signing and encrypting are separate goals: the signature proves origin/integrity; encryption keeps the contents secret.

9. **15 %**

   Error rate = $6 \,/\, 40 \times 100 = 15\%$.

10. **digest**

    The same input always gives the same digest, a small change gives a completely different one, and the input cannot be recovered from it.