17. Security

Starter Quiz · 课前小测

A-Level Computer Science Name: _____ Score: _____

1. Symmetric encryption uses:

   ☐ the same key to encrypt and decrypt

   ☐ a public key and a private key

   ☐ no key at all

   ☐ a one-way hash

2. TLS provides which combination of protections for data in transit?

   ☐ encryption, authentication and integrity

   ☐ compression only

   ☐ faster downloads only

   ☐ spam filtering

3. To send a confidential message to Alice using asymmetric encryption, you encrypt with:

   ☐ Alice's public key (only her private key can decrypt it)

   ☐ Alice's private key

   ☐ your own private key

   ☐ a shared session key

4. Which protections does TLS provide for data in transit? Select **all** that apply.

   ☐ encryption, so an eavesdropper reads only ciphertext

   ☐ authentication of the server's identity

   ☐ integrity, so tampering in transit is detected

   ☐ a guarantee that the data will arrive

   Tick every correct option.

5. Bob sends Alice a confidential message using asymmetric encryption. Which key does he encrypt with?

   ☐ Alice's public key

   ☐ Bob's public key

   ☐ Bob's private key

   ☐ Alice's private key

6. When verifying a certificate, the client checks that it is:

   ☐ in date, matches the URL, and signed by a trusted CA

   ☐ the largest certificate available

   ☐ written in the right language

   ☐ stored on the user's disk

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

   _____

8. A cryptographic hash is one-way (you cannot recover the input from the digest) and shows the avalanche effect — a tiny change in the input flips a large, unpredictable part of the output.

   ☐ True ☐ False

9. 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

10. Why store passwords as hashes rather than encrypted? Select **all** that apply.

    ☐ hashing is one-way, so a stolen database does not yield the passwords

    ☐ encryption is reversible, and an attacker may obtain the key too

    ☐ login still works by comparing digests of what the user typed

    ☐ hashing makes the passwords shorter to store

    Tick every correct option.

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. **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.

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

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

5. **Alice's public key**

   Only Alice's private key can undo what her public key did, and only Alice has it. Bob never sees Alice's private key at all.

6. **in date, matches the URL, and signed by a trusted CA**

   The browser checks validity dates, that the subject name matches the site, and the CA signature up to a trusted root.

7. **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.

8. **True**

   One-wayness plus avalanche is what makes hashes good for storing passwords and checking integrity.

9. **True**

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

10. **hashing is one-way, so a stolen database does not yield the passwords; encryption is reversible, and an attacker may obtain the key too; login still works by comparing digests of what the user typed**

    A fixed-size digest may indeed be shorter, but that is not the security reason. Irreversibility is.