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. 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

5. In the hybrid approach used by HTTPS, asymmetric encryption is used to:

   ☐ securely exchange a session key, which is then used with fast symmetric encryption

   ☐ encrypt all the data, because it is fastest

   ☐ replace hashing

   ☐ store passwords

6. 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

7. 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

8. To create a digital signature, the sender:

   ☐ hashes the message and encrypts the hash with their private key

   ☐ encrypts the message with the receiver's public key

   ☐ shares their private key

   ☐ compresses the message

17. Security

Answers · 答案

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. **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.

5. **securely exchange a session key, which is then used with fast symmetric encryption**

   Slow asymmetric crypto just shares a session key; the bulk data then uses fast symmetric encryption.

6. **True**

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

7. **True**

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

8. **hashes the message and encrypts the hash with their private key**

   Signing = hash the message, then encrypt the digest with the private key; the receiver verifies with the public key.