

< Previous

Unit 6 of 7 ▾

Next >

✓ 200 XP ➔

Knowledge check

1 minute

Choose the best response for each of the questions below. Then select "Check your answers".

Check your knowledge

1. How many keys are required when using symmetric encryption?

- Three.
- One.

✓ That's correct. Symmetric encryption uses one secret encryption key that's shared with all parties.

- Two.

2. When using asymmetric encryption, which key shouldn't be shared?

- Private key.

✓ That's correct. The private key should always be kept safe and never shared.

- Public key.
- Key pair.

3. What is a hashing function?

- A hashing function is an algorithm that creates a new ciphertext message from the plaintext.
 - A hashing function is an algorithm that's used to decrypt ciphertext from the sender.
 - A hashing function is an algorithm that creates a fixed-length hexadecimal value of the plaintext.
- ✓ That's correct. The hashing function creates a value that represents the content of plaintext and can be used to verify that the source document hasn't changed.**
-

Next unit: Summary and resources

[Continue >](#)
