Cryptography Fundamentals

Cryptography · Answer Key · 8 Questions

1. Which algorithm is widely considered the first to use a public-key (asymmetric) cryptosystem?

A) AES
B) RSA
C) DES
D) MD5

2. What does the acronym 'AES' stand for in modern data encryption?

A) Advanced Encryption Standard
B) Automatic Encoding System
C) Applied Electronic Security
D) Asymmetric Encryption Suite

3. In symmetric-key cryptography, what is the primary requirement for secure communication?

A) Multiple public keys
B) A secure digital certificate
C) The sender and receiver share the same secret key
D) An internet connection

4. What type of cryptographic function is designed to be one-way and produces a fixed-size string of characters regardless of input size?

A) Hash function
B) Digital signature
C) Symmetric cipher
D) Asymmetric cipher

5. Which of the following is an example of a common hashing algorithm?

A) RSA
B) SHA-256
C) Diffie-Hellman
D) AES-128

6. What is the primary purpose of a digital signature in electronic communications?

A) To hide the content of the message
B) To verify the authenticity and integrity of the message
C) To compress the message for faster transmission
D) To generate a public key for the receiver

Quixly | This material was auto-generated. Quixly is not liable for errors or omissions. Visit quixlylearn.com to report corrections.

7. Which term describes the process of converting readable information into an unreadable format to prevent unauthorized access?

A) Decoding
B) Hashing
C) Encryption
D) Steganography

8. What was the primary weakness of the Caesar Cipher used in ancient times?

A) It was too slow
B) It was susceptible to frequency analysis
C) It required a computer to solve
D) It did not support numbers