



212-81^{Q&As}

EC-Council Certified Encryption Specialist (ECES)

Pass EC-COUNCIL 212-81 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/212-81.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Basic information theory is the basis for modern symmetric ciphers. Understanding the terminology of information theory is, therefore, important. If a single change of a single bit in the plaintext causes changes in all the bits of the resulting ciphertext, what is this called?

- A. Complete diffusion
- B. Complete scrambling
- C. Complete confusion
- D. Complete avalanche

Correct Answer: D

QUESTION 2

Which of the following is an asymmetric cipher?

- A. RSA
- B. AES
- C. DES
- D. RC4

Correct Answer: A

RSA

[https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))

RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who

publicly described the algorithm in 1977. An equivalent system was developed secretly, in 1973 at GCHQ (the British signals intelligence agency), by the English mathematician Clifford Cocks. That system was declassified in 1997.

In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value.

The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

QUESTION 3

Which one of the following attempts to hide data in plain view?



- A. Cryptography
- B. Substitution
- C. Steganography
- D. Asymmetric cryptography

Correct Answer: C

Steganography <https://en.wikipedia.org/wiki/Steganography> Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography comes from Greek steganographia, which combines the words steganos , meaning "covered or concealed", and -graphia meaning "writing".

QUESTION 4

In relationship to hashing, the term _____ refers to random bits that are used as one of the inputs to the hash. Essentially the _____ is intermixed with the message that is to be hashed

- A. Vector
- B. Salt
- C. Stream
- D. IV

Correct Answer: B

Salt

[https://en.wikipedia.org/wiki/Salt_\(cryptography\)](https://en.wikipedia.org/wiki/Salt_(cryptography))

A salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but

over time additional safeguards were developed to protect a user's password against being read from the system. A salt is one of those methods.

QUESTION 5

Denis is looking at an older system that uses DES encryption. A colleague has told him that DES is insecure due to a small key size. What is the key length used for DES?

- A. 128
- B. 256
- C. 56
- D. 64



Correct Answer: C

<https://en.wikipedia.org/wiki/DES>

The Data Encryption Standard is a symmetric-key algorithm for the encryption of digital data. Although its short key length of 56 bits makes it too insecure for applications, it has been highly influential in the advancement of cryptography.

[Latest 212-81 Dumps](#)

[212-81 VCE Dumps](#)

[212-81 Practice Test](#)