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.leads4pass.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

QUESTION 1

Asymmetric encryption method developed in 1984. It is used in PGP implementations and GNU Privacy Guard Software. Consists of 3 parts: key generator, encryption algorithm, and decryption algorithm.

A. Tiger

B. GOST

C. RIPEMD

D. ElGamal

Correct Answer: D

ElGamal https://en.wikipedia.org/wiki/ElGamal_encryption the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key exchange. It was described by Taher Elgamal in 1985. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm (DSA) is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption.

QUESTION 2

Which of the following algorithms uses three different keys to encrypt the plain text?

A. Skipjack

B. AES

C. Blowfish

D. 3DES

Correct Answer: D

3DES https://en.wikipedia.org/wiki/Triple_DES Triple DES (3DES) has a three different keys with same size (56-bit).

QUESTION 3

Fred is using an operating system that stores all passwords as an MD5 hash. What size is an MD5 message digest (hash)?

A. 160

B. 512

C. 256

D. 128

Correct Answer: D

https://en.wikipedia.org/wiki/MD5

The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value.

QUESTION 4

Which of the following is a fundamental principle of cryptography that holds that the algorithm can be publicly disclosed without damaging security?

A. Vigenere\\'s principle

B. Shamir\\'s principle

C. Kerkchoff\\'s principle

D. Babbage\\'s principle

Correct Answer: C

Kerkchoff\\'s principle https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle Kerckhoffs\\'s principle (also called Kerckhoffs\\'s desideratum, assumption, axiom, doctrine or law) of cryptography was stated by Netherlands born cryptographer Auguste Kerckhoffs in the 19th century: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge. Kerckhoffs\\'s principle was reformulated (or possibly independently formulated) by American mathematician Claude Shannon as "the enemy knows the system", i.e., "one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them". In that form, it is called Shannon\\'s maxim. This concept is widely embraced by cryptographers, in contrast to "security through obscurity", which is not.

QUESTION 5

A _____ refers to a situation where two different inputs yield the same output.

A. Convergence

B. Collision

C. Transposition

D. Substitution

Correct Answer: B

Collision

https://en.wikipedia.org/wiki/Collision_(computer_science) A collision or clash is a situation that occurs when two distinct pieces of data have the same hash value, checksum, fingerprint, or cryptographic digest.