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.pass4itsure.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

Which of the following is not a key size used by AES?

A. 128 bits

B. 192 bits

C. 256 bits

D. 512 b

Correct Answer: D

512 bits https://en.wikipedia.org/wiki/Advanced_Encryption_Standard AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

QUESTION 2

Changing some part of the plain text for some matching part of cipher text. Historical algorithms typically use this.

A. Decoding

B. Substitution

C. Transposition

D. Collision

Correct Answer: B

Substitution

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

In cryptography, a substitution cipher is a method of encrypting by which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters,

mixtures of the above, and so forth. The receiver deciphers the text by performing the inverse substitution.

QUESTION 3

RFC 1321 describes what hash?

A. RIPEMD

B. GOST

C. SHA1

D. MD5

Correct Answer: D

MD5 https://en.wikipedia.org/wiki/MD5 MD5 was designed by Ronald Rivest in 1991 to replace an earlier hash function MD4, and was specified in 1992 as RFC 1321.

QUESTION 4

A _______ product refers to an NSA-endorsed classified or controlled cryptographic item for classified or sensitive U. S. government information, including cryptographic equipment, assembly, or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed

A. 1

B. 4

C. 2

D. 3

Correct Answer: A

Type 1 https://en.wikipedia.org/wiki/NSA_cryptography#Type_1_Product A Type 1 Product refers to an NSA endorsed classified or controlled cryptographic item for classified or sensitive U.S. government information, including cryptographic equipment, assembly or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed.

QUESTION 5

WPA2 uses AES for wireless data encryption at which of the following encryption levels?

A. 128 bit and CRC

B. 128 bi and TKIP

C. 128 bit and CCMP

D. 64 bit and CCMP

Correct Answer: C

128 bit and CCMP

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol that forms part of the 802.11i standard for wireless local area networks (WLANs), particularly those using WiMax technology.

CCMP employs 128-bit keys and a 48-bit initialization vector that minimizes vulnerability to replay attacks.