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.geekcert.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

John is responsible for VPNs at his company. He is using IPSec because it has two different modes. He can choose the mode appropriate for a given situation. What are the two modes of IPSec? (Choose two)

A. Encrypt mode

B. Transport mode

C. Tunnel mode

D. Decrypt mode

Correct Answer: BC

Correct answers: Transport mode and Tunnel mode

https://en.wikipedia.org/wiki/IPsec#Modes_of_operation The IPsec protocols AH and ESP can be implemented in a host-to-host transport mode, as well as in a network tunneling mode.

QUESTION 2

Which of the following asymmetric algorithms is described by U.S. Patent 5,231,668 and FIPS 186?

A. AES

B. RC4

C. DSA

D. RSA

Correct Answer: C

DSA https://ru.wikipedia.org/wiki/DSA The National Institute of Standards and Technology (NIST) proposed DSA for use in their Digital Signature Standard (DSS) in 1991, and adopted it as FIPS 186 in 1994. DSA is covered by U.S. Patent 5,231,668 , filed July 26, 1991 and now expired, and attributed to David W. Kravitz, a former NSA employee.

QUESTION 3

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.

QUESTION 4

If you wished to see a list of revoked certificates from a CA, where would you look?

A. RA

B. RFC

C. CRL

D. CA

Correct Answer: C

CRL https://ru.wikipedia.org/wiki/Certificate_Revocation_List Certificate Revocation List (or CRL) is "a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date and should no longer be trusted".

QUESTION 5

Ahlen is using a set of pre-calculated hashes to attempt to derive the passwords from a Windows SAM file. What is a set of pre-calculated hashes used to derive a hashed password called?

A. Hash matrix

B. Rainbow table

C. Password table

D. Hash table

Correct Answer: B

Rainbow table https://en.wikipedia.org/wiki/Rainbow_table A rainbow table is a precomputed table for caching the output of cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a key derivation function (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters. It is a practical example of a space-time tradeoff, using less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple key derivation function with one entry per hash. Use of a key derivation that employs a salt makes this attack infeasible.