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

Ferris has been assigned the task of selecting security for his company\\'s wireless network. It is important that he pick the strongest form of wireless security. Which one of the following is the strongest wireless security?

A. WEP

B. WPA

C. WPA2

D. TKIP

Correct Answer: C

WPA2 https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access WPA (sometimes referred to as the draft IEEE 802.11i standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2, which became available in 2004 and is a common shorthand for the full IEEE 802.11i (or IEEE 802.11i-2004) standard.

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)

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

Ciphers that write message letters out diagonally over a number of rows then read off cipher row by row. Also called zig-zag cipher.

A. Rail Fence Cipher

B. Null Cipher

C. Vigenere Cipher

D. ROT-13

Correct Answer: A

Rail Fence Cipher https://en.wikipedia.org/wiki/Rail_fence_cipher The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded.

QUESTION 4

Juanita has been assigned the task of selecting email encryption for the staff of the insurance company she works for. The various employees often use diverse email clients. Which of the following methods is available as an add-in for most email clients?

A. Caesar cipher

B. RSA

C. PGP

D. DES

Correct Answer: C

PGP https://en.wikipedia.org/wiki/Pretty_Good_Privacy Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. Phil Zimmermann developed PGP in 1991.

QUESTION 5

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.