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

QUESTION 1

What advantage do symmetric algorithms have over asymmetric algorithms

A. It is easier to implement them in software

B. They are more secure

C. They are faster

D. It is easier to exchange keys

Correct Answer: C

They are faster

Symmetric key encryption is much faster than asymmetric key encryption, because both the sender and the recipient of a message to use the same secret key.

QUESTION 2

Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?

A. Key distribution

B. Security

C. Scalability

D. Speed

Correct Answer: D

Speed

Symmetric key systems are considerably faster than asymmetric key systems but have issues with proper key distribution, controlling keys as more users need to communicate, and cannot provide non-repudiation or authenticity.

QUESTION 3

In IPSec, if the VPN is a gateway-gateway or a host-gateway, then which one of the following is true?

A. IPSec does not involve gateways

B. Only transport mode can be used

C. Encapsulating Security Payload (ESP) authentication must be used

D. Only the tunnel mode can be used

Correct Answer: D

IPSec has two different modes: transport mode and tunnel mode.

Only the tunnel mode can be used

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

In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create virtual private networks for network-to-network communications (e.g.

between routers to link sites), host- to-network communications (e.g. remote user access) and host-to-host communications (e.g. private chat).

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

All of the following are key exchange protocols except for____

A. MQV

B. AES

C. ECDH

D. DH

Correct Answer: B

Latest 212-81 Dumps 212-81 Practice Test 212-81 Study Guide