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

Which of the following is a type of encryption that has two different keys. One key can encrypt the message and the other key can only decrypt it?

A. Block cipher

B. Asymmetric

C. Symmetric

D. Stream cipher

Correct Answer: B

Asymmetric Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys, which may be disseminated widely, and private keys, which are known only to the owner. The generation of such keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.

QUESTION 2

Basic information theory is the basis for modern symmetric ciphers. Understanding the terminology of information theory is, therefore, important. Changes to one character in the plaintext affect multiple characters in the ciphertext. What is this referred to?

A. Avalanche

B. Confusion

C. Scrambling

D. Diffusion

Correct Answer: D

Diffusion https://en.wikipedia.org/wiki/Confusion_and_diffusion Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change. Since a bit can have only two states, when they are all re-evaluated and changed from one seemingly random position to another, half of the bits will have changed state. The idea of diffusion is to hide the relationship between the ciphertext and the plain text. This will make it hard for an attacker who tries to find out the plain text and it increases the redundancy of plain text by spreading it across the rows and columns; it is achieved through transposition of algorithm and it is used by block ciphers only

---

QUESTION 3

Which of the following is a block cipher?

A. AES

B. DH

C. RC4

D. RSA

Correct Answer: A

AES 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

QUESTION 4

Terrance oversees the key escrow server for his company. All employees use asymmetric cryptography to encrypt all emails. How many keys are needed for asymmetric cryptography?

A. 2

B. 4

C. 3

D. 1

Correct Answer: A

https://en.wikipedia.org/wiki/Public-key_cryptography Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys, which may be disseminated widely, and private keys, which are known only to the owner. The generation of such keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.

In such a system, any person can encrypt a message using the receiver\\'s public key, but that encrypted message can only be decrypted with the receiver\\'s private key.

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.