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

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

Which of the following would be the weakest encryption algorithm?

A. DES

B. AES

C. RSA

D. EC

Correct Answer: A

DES https://en.wikipedia.org/wiki/Data_Encryption_Standard DES is insecure due to the relatively short 56-bit key size. In January 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes.

QUESTION 2

A simple algorithm that will take the initial key and from that generate a slightly different key each round.

A. Key Schedule

B. Feistel Network

C. SHA-2

D. Diffie-Helman

Correct Answer: A

Key Schedule https://en.wikipedia.org/wiki/Key_schedule In cryptography, the so-called product ciphers are a certain kind of cipher, where the (de-)ciphering of data is typically done as an iteration of rounds. The setup for each round is generally the same, except for round-specific fixed values called a round constant, and round-specific data derived from the cipher key called a round key. A key schedule is an algorithm that calculates all the round keys from the key.

QUESTION 3

A measure of the uncertainty associated with a random variable.

A. Collision

B. Whitening

C. Diffusion

D. Entropy

Correct Answer: D

Entropy https://en.wikipedia.org/wiki/Entropy_(information_theory) In information theory, the entropy of a random variable is the average level of "information", "surprise", or "uncertainty" inherent in the variable\\'s possible outcomes. The concept of information entropy was introduced by Claude Shannon in his 1948 paper "A Mathematical Theory of Communication".

QUESTION 4

With Electronic codebook (ECB) what happens:

A. The message is divided into blocks and each block is encrypted separately. This is the most basic mode for symmetric encryption

B. The cipher text from the current round is XORed with the plaintext from the previous round

C. The block cipher is turned into a stream cipher

D. The cipher text from the current round is XORed with the plaintext for the next round

Correct Answer: A

The message is divided into blocks and each block is encrypted separately. This is the most basic mode for symmetric encryption

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Electronic_codebook_(ECB)

The simplest of the encryption modes is the electronic codebook (ECB) mode (named after conventional physical codebooks). The message is divided into blocks, and each block is encrypted separately.

QUESTION 5

Which one of the following is an example of a symmetric key algorithm?

A. ECC

B. Diffie-Hellman

C. RSA

D. Rijndael

Correct Answer: D

Rijndael https://en.wikipedia.org/wiki/Advanced_Encryption_Standard The Advanced Encryption Standard (AES), also known by its original name Rijndael. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

212-81 VCE Dumps 212-81 Exam Questions 212-81 Braindumps