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

In relationship to hashing, the term _____refers to random bits that are used as one of the inputs to the hash. Essentially the _____ is intermixed with the message that is to be hashed

A. Vector

B. Salt

C. Stream

D. IV

Correct Answer: B

Salt

https://en.wikipedia.org/wiki/Salt_(cryptography)

A salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but

over time additional safeguards were developed to protect a user\\'s password against being read from the system. A salt is one of those methods.

QUESTION 2

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.

QUESTION 3

What size block does Skipjack use?

A. 64

B. 512

C. 128

D. 256

Correct Answer: A

https://en.wikipedia.org/wiki/Skipjack_(cipher)

Skipjack uses an 80-bit key to encrypt or decrypt 64-bit data blocks. It is an unbalanced Feistel network with 32 rounds.

QUESTION 4

Which one of the following attempts to hide data in plain view?

A. Cryptography

B. Substitution

C. Steganography

D. Asymmetric cryptography

Correct Answer: C

Steganography https://en.wikipedia.org/wiki/Steganography Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography comes from Greek steganographia, which combines the words steganos , meaning "covered or concealed", and -graphia meaning "writing".

QUESTION 5

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.