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

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

QUESTION 1

A _____ is a function is not reversible.

A. Stream cipher

B. Asymmetric cipher

C. Hash

D. Block Cipher

Correct Answer: C

Hash https://en.wikipedia.org/wiki/Hash_function Hash functions are irreversible. This is actually required for them to fulfill their function of determining whether someone possesses an uncorrupted copy of the hashed data. This brings susceptibility to brute force attacks, which are quite powerful these days, particularly against MD5.

QUESTION 2

Algorithm that was chosen for the Data Encryption Standard, which was altered and renamed Data Encryption Algorithm.

A. Blowfish

B. Rijndael

C. Lucifer

D. El Gamal

Correct Answer: C

Lucifer

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

Lucifer was a direct precursor to the Data Encryption Standard. One version, alternatively named DTD-1.

QUESTION 3

A linear congruential generator is an example of what?

A. A coprime generator

B. A prime number generator

C. A pseudo random number generator

D. A random number generator

Correct Answer: C

A pseudo random number generator https://en.wikipedia.org/wiki/Linear_congruential_generator A linear congruential generator (LCG) is an algorithm that yields a sequence of pseudo- randomized numbers calculated with a discontinuous piecewise linear equation. The method represents one of the oldest and best-known pseudorandom number generator algorithms. The theory behind them is relatively easy to understand, and they are easily implemented and fast, especially on computer hardware which can provide modular arithmetic by storage-bit truncation.

QUESTION 4

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 5

_____ uses at least two different shifts, changing the shift with different letters in the plain text.

A. Caesar cipher

B. multi-alphabet encryption

C. Scytale

D. Atbash

Correct Answer: B

multi-alphabet encryption https://en.wikipedia.org/wiki/Polyalphabetic_cipher Two different shifts create two different alphabets. For +1 and +2 Plaintext alphabet A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 2 ciphertext alphabets B C D E F G H I J K L M N O P Q R S T U V W X Y Z A C D E F G H I J K L M N O P Q R S T U V W X Y Z A B