212-81$^{\text{Q\&As}}$

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

Which of the following was a multi alphabet cipher widely used from the 16th century to the early 20th century?

A. Atbash

B. Caesar

C. Scytale

D. Vigenere

Correct Answer: D

QUESTION 2

A ______ refers to a situation where two different inputs yield the same output.

A. Convergence

B. Collision

C. Transposition

D. Substitution

Correct Answer: B

Collision

https://en.wikipedia.org/wiki/Collision_(computer_science) A collision or clash is a situation that occurs when two distinct pieces of data have the same hash value, checksum, fingerprint, or cryptographic digest.

QUESTION 3

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 4

Represents the total number of possible values of keys in a cryptographic algorithm or other security measure, such as a password.

A. Key Schedule

B. Key Clustering

C. Key Space

D. Key Exchange

Correct Answer: C

Key Space https://en.wikipedia.org/wiki/Key_space_(cryptography) Algorithm\\'s key space refers to the set of all possible permutations of a key. To prevent an adversary from using a brute-force attack to find the key used to encrypt a message, the key space is usually designed to be large enough to make such a search infeasible. On average, half the key space must be searched to find the solution. Another desirable attribute is that the key must be selected truly randomly from all possible key permutations. Should this not be the case, and the attacker is able to determine some factor that may influence how the key was selected, the search space (and hence also the search time) can be significantly reduced. Humans do not select passwords randomly, therefore attackers frequently try a dictionary attack before a brute force attack, as this approach can often produce the correct answer in far less time than a systematic brute force search of all possible character combinations.

QUESTION 5

Basic information theory is the basis for modern symmetric ciphers. Understanding the terminology of information theory is, therefore, important. If a single change of a single bit in the plaintext causes changes in all the bits of the resulting ciphertext, what is this called?

A. Complete diffusion

B. Complete scrambling

C. Complete confusion

D. Complete avalanche

Correct Answer: D