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 transposition cipher invented 1918 by Fritz Nebel, used a 36 letter alphabet and a modified Polybius square with a single columnar transposition.

A. ADFVGX Cipher

B. ROT13 Cipher

C. Book Ciphers

D. Cipher Disk

Correct Answer: A

ADFVGX Cipher https://en.wikipedia.org/wiki/ADFGVX_cipher ADFGVX cipher was a field cipher used by the German Army on the Western Front during World War I. ADFGVX was in fact an extension of an earlier cipher called ADFGX. Invented by Lieutenant Fritz Nebel (1891?977) and introduced in March 1918, the cipher was a fractionating transposition cipher which combined a modified Polybius square with a single columnar transposition.

QUESTION 2

Frank is trying to break into an encrypted file... He is attempting all the possible keys that could be used for this algorithm. Attempting to crack encryption by simply trying as many randomly generated keys as possible is referred to as what?

A. Rainbow table

B. Frequency analysis

C. Brute force

D. Kasiski

Correct Answer: C

Brute force

https://en.wikipedia.org/wiki/Brute-force_attack

Brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.

QUESTION 3

RFC 1321 describes what hash?

A. RIPEMD

B. GOST

C. SHA1

D. MD5

Correct Answer: D

MD5 https://en.wikipedia.org/wiki/MD5 MD5 was designed by Ronald Rivest in 1991 to replace an earlier hash function MD4, and was specified in 1992 as RFC 1321.

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

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.

Latest 212-81 Dumps 212-81 Practice Test 212-81 Exam Questions