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.pass4itsure.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

John works as a cryptography consultant. He finds that people often misunderstand the reality of breaking a cipher. What is the definition of breaking a cipher?

A. Finding any method that is more efficient than brute force

B. Uncovering the algorithm used

C. Rendering the cypher no longer useable

D. Decoding the key

Correct Answer: A

Finding any method that is more efficient than brute force.

https://en.wikipedia.org/wiki/Cryptanalysis

Bruce Schneier notes that even computationally impractical attacks can be considered breaks: "Breaking a cipher simply means finding a weakness in the cipher that can be exploited with a complexity less than brute force. Never mind that

brute-force might require 2^128 encryptions; an attack requiring 2^110 encryptions would be considered a break...simply put, a break can just be a certificational weakness: evidence that the cipher does not perform as advertised."

QUESTION 2

The reverse process from encoding - converting the encoded message back into its plaintext format.

A. Substitution

B. Whitening

C. Encoding

D. Decoding

Correct Answer: D

Decoding

Decoding - reverse process from encoding,converting the encoded message back into its plaintext format.

QUESTION 3

Ciphers that write message letters out diagonally over a number of rows then read off cipher row by row. Also called zig-zag cipher.

A. Rail Fence Cipher

B. Null Cipher

C. Vigenere Cipher

D. ROT-13

Correct Answer: A

Rail Fence Cipher https://en.wikipedia.org/wiki/Rail_fence_cipher The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded.

QUESTION 4

Fred is using an operating system that stores all passwords as an MD5 hash. What size is an MD5 message digest (hash)?

A. 160

B. 512

C. 256

D. 128

Correct Answer: D

https://en.wikipedia.org/wiki/MD5

The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value.

QUESTION 5

Which of the following is generally true about key sizes?

A. Larger key sizes increase security

B. Key size is irrelevant to security

C. Key sizes must be more than 256 bits to be secure

D. Smaller key sizes increase security

Correct Answer: A

Larger key sizes increase security https://en.wikipedia.org/wiki/Key_size Key length defines the upper-bound on an algorithm\\'s security (i.e. a logarithmic measure of the fastest known attack against an algorithm), since the security of all algorithms can be violated by brute-force attacks. Ideally, the lower-bound on an algorithm\\'s security is by design equal to the key length (that is, the security is determined entirely by the keylength, or in other words, the algorithm\\'s design doesn\\'t detract from the degree of security inherent in the key length). Indeed, most symmetric-key algorithms are designed to have security equal to their key length. However, after design, a new attack might be discovered. For instance, Triple DES was designed to have a 168 bit key, but an attack of complexity 2112 is now known (i.e. Triple DES now only has 112 bits of security, and of the 168 bits in the key the attack has rendered 56 \\'ineffective\\' towards security). Nevertheless, as long as the security (understood as \\'the amount of effort it would take to gain access\\') is

sufficient for a particular application, then it doesn\\'t matter if key length and security coincide. This is important for asymmetric-key algorithms, because no such algorithm is known to satisfy this property; elliptic curve cryptography comes the closest with an effective security of roughly half its key length.