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

Protocol suite provides a method of setting up a secure channel for protected data exchange between two devices.

A. CLR

B. OCSP

C. TLS

D. IPSec

Correct Answer: D

IPSec https://en.wikipedia.org/wiki/IPsec Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).

QUESTION 2

Which of the following would be the weakest encryption algorithm?

A. DES

B. AES

C. RSA

D. EC

Correct Answer: A

DES https://en.wikipedia.org/wiki/Data_Encryption_Standard DES is insecure due to the relatively short 56-bit key size. In January 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes.

QUESTION 3

You are studying classic ciphers. You have been examining the difference between single substitution and multi-substitution. Which one of the following is an example of a multi- alphabet cipher?

A. Rot13

B. Caesar

C. Atbash

D. Vigenere

Correct Answer: D

Vigenere https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher The Vigenere cipher is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It employs a form of polyalphabetic substitution. First described by Giovan Battista Bellaso in 1553, the cipher is easy to understand and implement, but it resisted all attempts to break it until 1863, three centuries later. This earned it the description le chiffre indehiffrable (French for \\'the indecipherable cipher\\'). Many people have tried to implement encryption schemes that are essentially Vigenre ciphers. In 1863, Friedrich Kasiski was the first to publish a general method of deciphering Vigenre ciphers.

QUESTION 4

What best describes the shifting of each letter a fixed number of spaces to the left or right?

A. Single substitution

B. Multi substitution

C. XOR

D. Bit shifting

Correct Answer: A

Single substitution https://en.wikipedia.org/wiki/Substitution_cipher#Simple_substitution Substitution of single letters separately--simple substitution--can be demonstrated by writing out the alphabet in some order to represent the substitution. This is termed a substitution alphabet. The cipher alphabet may be shifted or reversed (creating the Caesar and Atbash ciphers, respectively) or scrambled in a more complex fashion, in which case it is called a mixed alphabet or deranged alphabet.

QUESTION 5

In a Feistel cipher, the two halves of the block are swapped in each round. What does this provide?

A. Diffusion

B. Confusion

C. Avalanche

D. Substitution

Correct Answer: B

Confusion https://en.wikipedia.org/wiki/Confusion_and_diffusion#Definition Confusion means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two. The property of confusion hides the relationship between the ciphertext and the key. This property makes it difficult to find the key from the ciphertext and if a single bit in a key is changed, the calculation of the values of most or all of the bits in the ciphertext will be affected. Confusion increases the ambiguity of ciphertext and it is used by both block and stream ciphers.

Incorrect answer: Avalanche - The avalanche effect is the desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions, wherein if an input is changed slightly (for example, flipping a single bit), the output changes significantly (e.g., half the output bits flip). In the case of high-quality block ciphers, such a small change in either the key or the plaintext should cause a drastic change in the ciphertext. The actual term was first used by Horst

Feistel, although the concept dates back to at least Shannon\\'s diffusion. Diffusion - Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change.[2] Since a bit can have only two states, when they are all re-evaluated and changed from one seemingly random position to another, half of the bits will have changed state. Substitution - Substitution technique is a classical encryption technique where the characters present in the original message are replaced by the other characters or numbers or by symbols.