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

What is a variation of DES that uses a technique called Key Whitening?

A. Blowfish

B. DESX

C. 3DES

D. AES

Correct Answer: B

DESX https://en.wikipedia.org/wiki/DES-X In cryptography, DES-X (or DESX) is a variant on the DES (Data Encryption Standard) symmetric-key block cipher intended to increase the complexity of a brute-force attack using a technique called key whitening.

QUESTION 2

Electromechanical rotor-based cipher used in World War II

A. ROT13 Cipher

B. Cipher Disk

C. Enigma Machine

D. Rail Fence Cipher

Correct Answer: C

Enigma Machine https://en.wikipedia.org/wiki/Enigma_machine The Enigma machine is an encryption device developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication. It was employed extensively by Nazi Germany during World War II, in all branches of the German military. Enigma has an electromechanical rotor mechanism that scrambles the 26 letters of the alphabet.

QUESTION 3

As a network administrator, you have implemented WPA2 encryption in your corporate wireless network. The WPA2\\'s _____ integrity check mechanism provides security against a replay attack.

A. CBC-MAC

B. CRC-MAC

C. CRC-32

D. CBC-32

Correct Answer: A

CBC-MAC https://en.wikipedia.org/wiki/CBC-MAC A cipher block chaining message authentication code (CBC-MAC) is a technique for constructing a message authentication code from a block cipher. The message is encrypted with some block cipher algorithm in CBC mode to create a chain of blocks such that each block depends on the proper encryption of the previous block. This interdependence ensures that a change to any of the plaintext bits will cause the final encrypted block to change in a way that cannot be predicted or counteracted without knowing the key to the block cipher. Using in WPA2 for integrity check and provides security against a replay attack.

QUESTION 4

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.

QUESTION 5

Part of understanding cryptography is understanding the cryptographic primitives that go into any crypto system. A(n) _____ is a fixed-size input to a cryptographic primitive that is random or pseudorandom.

A. Key

B. IV

C. Chain

D. Salt

Correct Answer: A

Key

https://en.wikipedia.org/wiki/Key_(cryptography)

In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm. For encryption algorithms, a key specifies the transformation of plaintext into ciphertext, and vice versa for

decryption algorithms. Keys also specify transformations in other cryptographic algorithms, such as digital signature schemes and message authentication codes.