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

DES has a key space of what?

A. 2^128

B. 2^192

C. 2^64

D. 2^56

Correct Answer: D

2^56 https://en.wikipedia.org/wiki/Data_Encryption_Standard The Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of digital data. Although its short key length of 56 bits makes it too insecure for applications, it has been highly influential in the advancement of cryptography.

QUESTION 2

Which of the following is the successor of SSL?

A. GRE

B. RSA

C. IPSec

D. TLS

Correct Answer: D

TLS

https://en.wikipedia.org/wiki/Transport_Layer_Security#History_and_development TLS 1.0 was first defined in RFC 2246 in January 1999 as an upgrade of SSL Version 3.0, and written by Christopher Allen and Tim Dierks of Consensus

Development. As stated in the RFC, "the differences between this protocol and SSL 3.0 are not dramatic, but they are significant enough to preclude interoperability between TLS 1.0 and SSL 3.0". Tim Dierks later wrote that these changes,

and the renaming from "SSL" to "TLS", were a face-saving gesture to Microsoft, "so it wouldn\\'t look [like] the IETF was just rubberstamping Netscape\\'s protocol".

QUESTION 3

Collision resistance is an important property for any hashing algorithm. Joan wants to find a cryptographic hash that has strong collision resistance. Which one of the following is the most collisionresistant?

A. SHA2

B. MD5

C. MD4

D. PIKE

Correct Answer: A

SHA2 https://en.wikipedia.org/wiki/Collision_resistance Collision resistance is a property of cryptographic hash functions: a hash function H is collision-resistant if it is hard to find two inputs that hash to the same output; that is, two inputs a and b where a b but H(a) = H(b). The pigeonhole principle means that any hash function with more inputs than outputs will necessarily have such collisions; the harder they are to find, the more cryptographically secure the hash function is. Due to the Birthday Problem, for a hash function that produces an output of length n bits, the probability of getting a collision is 1/2^n/2. So, just looking for a hash function with larger "n". The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA- 512/256.

QUESTION 4

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 5

A cryptanalysis success where the attacker discovers additional plain texts (or cipher texts) not previously known.

A. Total Break

B. Distinguishing Algorithm

C. Instance Deduction

D. Information Deduction

Correct Answer: C

Instance Deduction

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

The results of cryptanalysis can also vary in usefulness. For example, cryptographer Lars Knudsen (1998) classified various types of attack on block ciphers according to the amount and quality of secret information that was discovered:

Total break -- the attacker deduces the secret key. Global deduction -- the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key. Instance (local) deduction -- the attacker discovers

additional plaintexts (or ciphertexts) not previously known.

Information deduction -- the attacker gains some Shannon information about plaintexts (or ciphertexts) not previously known.

Distinguishing algorithm -- the attacker can distinguish the cipher from a random permutation.