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

Hash algortihm created by the Russians. Produces a fixed length output of 256bits. Input message is broken up into 256 bit blocks. If block is less than 256 bits then it is padded with 0s.

A. TIGER

B. GOST

C. BEAR

D. FORK-256

Correct Answer: B

GOST https://en.wikipedia.org/wiki/GOST_(hash_function) The GOST hash function, defined in the standards GOST R 34.11-94 and GOST 34.311- 95 is a 256-bit cryptographic hash function. It was initially defined in the Russian national standard GOST R 34.11-94 Information Technology ?Cryptographic Information Security ?Hash Function. The equivalent standard used by other member-states of the CIS is GOST 34.311-95.

QUESTION 2

If the round function is a cryptographically secure pseudorandom function, then _____ rounds is sufficient to make the block cipher a pseudorandom permutation.

A. 2

B. 15

C. 16

D. 3

Correct Answer: D

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

Michael Luby and Charles Rackoff analyzed the Feistel cipher construction, and proved that if the round function is a cryptographically secure pseudorandom function, with Ki used as the seed, then 3 rounds are sufficient to make the block

cipher a pseudorandom permutation, while 4 rounds are sufficient to make it a "strong" pseudorandom permutation (which means that it remains pseudorandom even to an adversary who gets oracle access to its inverse permutation).

Because of this very important result of Luby and Rackoff, Feistel ciphers are sometimes called Luby-Rackoff block ciphers.

QUESTION 3

All of the following are key exchange protocols except for____

A. MQV

B. AES

C. ECDH

D. DH

Correct Answer: B

QUESTION 4

A _____ product refers to an NSA-endorsed classified or controlled cryptographic item for classified or sensitive U. S. government information, including cryptographic equipment, assembly, or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed

A. 1

B. 4

C. 2

D. 3

Correct Answer: A

Type 1 https://en.wikipedia.org/wiki/NSA_cryptography#Type_1_Product A Type 1 Product refers to an NSA endorsed classified or controlled cryptographic item for classified or sensitive U.S. government information, including cryptographic equipment, assembly or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed.

QUESTION 5

During the process of encryption and decryption, what keys are shared?

A. Public keys

B. Public and private keys

C. User passwords

D. Private keys

Correct Answer: A

Public keys https://en.wikipedia.org/wiki/Public-key_cryptography Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys, which may be disseminated widely, and private keys, which are known only to the owner. The generation of such keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security. In such a system, any person can encrypt a message using the receiver\\'s public key, but that encrypted message can only be decrypted with the receiver\\'s private key.

Alice and Bob have two keys of their own -- just to be clear, that\\'s four keys total. Each party has their own public key, which they share with the world, and their own private key which they well, which they keep private, of course but, more than that, which they keep as a closely guarded secret. The magic of public key cryptography is that a message encrypted with the public key can only be decrypted with the private key. Alice will encrypt her message with Bob\\'s public key, and even though Eve knows she used Bob\\'s public key, and even though Eve knows Bob\\'s public key herself, she is unable to decrypt the message. Only Bob, using his secret key, can decrypt the message assuming he\\'s kept it secret, of course.

Alice and Bob do not need to plan anything ahead of time to communicate securely: they generate their public-private key pairs independently, and happily broadcast their public keys to the world at large. Alice can rest assured that only Bob can decrypt the message she sends because she has encrypted it with his public key.