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.passapply.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 is going to use RSA to encrypt a message to Joan. What key should he use?

A. A random key

B. Joan\\'s public key

C. A shared key

D. Joan\\'s private key

Correct Answer: B

Joan\\'s public key https://en.wikipedia.org/wiki/RSA_(cryptosystem) Suppose Joahn uses Bob\\'s public key to send him an encrypted message. In the message, she can claim to be Alice but Bob has no way of verifying that the message was actually from Alice since anyone can use Bob\\'s public key to send him encrypted messages. In order to verify the origin of a message, RSA can also be used to sign a message. Suppose Alice wishes to send a signed message to Bob. She can use her own private key to do so. She produces a hash value of the message, raises it to the power of d (modulo n) (as she does when decrypting a message), and attaches it as a "signature" to the message. When Bob receives the signed message, he uses the same hash algorithm in conjunction with Alice\\'s public key. He raises the signature to the power of e (modulo n) (as he does when encrypting a message), and compares the resulting hash value with the message\\'s actual hash value. If the two agree, he knows that the author of the message was in possession of Alice\\'s private key, and that the message has not been tampered with since.

QUESTION 2

Which algorithm implements an unbalanced Feistel cipher?

A. Skipjack

B. RSA

C. 3DES

D. Blowfish

Correct Answer: A

Skipjack

https://en.wikipedia.org/wiki/Skipjack_(cipher)

Skipjack uses an 80-bit key to encrypt or decrypt 64-bit data blocks. It is an unbalanced Feistel network with 32 rounds.

QUESTION 3

Nicholas is working at a bank in Germany. He is looking at German standards for pseudo random number generators. He wants a good PRNG for generating symmetric keys. The German Federal Office for Information Security (BSI) has established four criteria for quality of random number generators. Which ones can be used for cryptography?

A. K4

B. K5

C. K3

D. K2

E. K1

Correct Answer: AC

QUESTION 4

What is the solution to the equation 8 mod 3?

A. 1

B. 4

C. 3

D. 2

Correct Answer: D

https://en.wikipedia.org/wiki/Modulo_operation The modulo operation returns the remainder or signed remainder of a division, after one number is divided by another (called the modulus of the operation). Given two positive numbers a and n, a modulo n (abbreviated as a mod n) is the remainder of the Euclidean division of a by n, where a is the dividend and n is the divisor. The modulo operation is to be distinguished from the symbol mod, which refers to the modulus (or divisor) one is operating from. For example, the expression "5 mod 2" would evaluate to 1, because 5 divided by 2 has a quotient of 2 and a remainder of 1, while "9 mod 3" would evaluate to 0, because the division of 9 by 3 has a quotient of 3 and a remainder of 0; there is nothing to subtract from 9 after multiplying 3 times 3.

QUESTION 5

RFC 1321 describes what hash?

A. RIPEMD

B. GOST

C. SHA1

D. MD5

Correct Answer: D

MD5 https://en.wikipedia.org/wiki/MD5 MD5 was designed by Ronald Rivest in 1991 to replace an earlier hash function MD4, and was specified in 1992 as RFC 1321.