Free Questions for 212-81 by dumpshq

Shared by Weeks on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which of the following is the successor of SSL?

Options:

A- GRE

B- RSA

C- IPSec

D- TLS

Answer:

D

Explanation:

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 2

Question Type: MultipleChoice

Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?

Options:

A- Key distribution

B- Security

C- Scalability

D- Speed

Answer:

D

Explanation:

Speed

Symmetric key systems are considerably faster than asymmetric key systems but have issues with proper key distribution, controlling keys as more users need to communicate, and cannot provide non-repudiation or authenticity.

Question 3

Question Type: MultipleChoice

Which one of the following wireless standards uses the Advanced Encryption Standard (AES) using the Counter Mode-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP)?

Options:

A- WEP

B- WEP2

C- WPA

D- WPA2

Answer:

D

Explanation:

WPA2

https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA2

WPA2 use the Counter Mode-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP).

Question 4

Question Type: **MultipleChoice**

A _______ refers to a situation where two different inputs yield the same output.

Options:

A- Convergence

B- Collision

C- Transposition

D- Substitution

Answer:

B

Explanation:

Collision

https://en.wikipedia.org/wiki/Collision_(computer_science)

A collision or clash is a situation that occurs when two distinct pieces of data have the same hash value, checksum, fingerprint, or cryptographic digest.

Question 5

Question Type: MultipleChoice

Which one of the following terms describes two numbers that have no common factors?

Options:

A- Coprime

B- Fermat's number

C- Euler's totient

D- Convergent

Answer:

A

Explanation:

Coprime

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

In number theory, two integers a and b are said to be relatively prime, mutually prime, or coprime if the only positive integer (factor) that divides both of them is 1. Consequently, any prime number that divides one of a or b does not divide the other. This is equivalent to their greatest common divisor (gcd) being 1.

Incorrect answers:

Convergent - a series is the sum of the terms of an infinite sequence of numbers.

Euler's totient function - counts the positive integers up to a given integer n that are relatively prime to n. It is written using the Greek letter phi as (n) or (n), and may also be called Euler's phi function. In other words, it is the number of integers k in the range 1 k n for which the greatest common divisor gcd(n, k) is equal to 1. The integers k of this form are sometimes referred to as totatives of n.

Fermat's number - named after Pierre de Fermat, who first studied them, is a positive integer of the form

where n is a non-negative integer.

Question 6

Question Type: MultipleChoice

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

Options:

A- Blowfish

B- DESX

C- 3DES

D- AES

Answer:

B

Explanation:

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 7

Question Type: **MultipleChoice**

Which algorithm implements an unbalanced Feistel cipher?

Options:

A- Skipjack

B- RSA

C- 3DES

D- Blowfish

Answer:

A

Explanation:

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 8

Question Type: **MultipleChoice**

Created by D. H. Lehmer. It is a classic example of a Linear congruential generator. A PRNG type of linear congruential generator (LCG) that operates in multiplicative group of integers modulo n. The basic algorithm is Xi+1=(aXi + c) mod m, with 0 Xi m.

Options:

A- Lehmer Random Number Generator

B- Lagged Fibonacci Generator

C- Linear Congruential Generator

D- Blum Blum Shub

Answer:

A

Explanation:

Lehmer Random Number Generator

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

The Lehmer random number generator (named after D. H. Lehmer), sometimes also referred to as the Park--Miller random number generator (after Stephen K. Park and Keith W. Miller), is a type of linear congruential generator (LCG) that operates in multiplicative group of integers modulo n. The general formula is:

where the modulus m is a prime number or a power of a prime number, the multiplier a is an element of high multiplicative order modulo m (e.g., a primitive root modulo n), and the seed X0 is coprime to m.

Other names are multiplicative linear congruential generator (MLCG) and multiplicative congruential generator (MCG).

Question 9

Question Type: MultipleChoice

RFC 1321 describes what hash?

Options:

A- RIPEMD

B- GOST

C- SHA1

D- MD5

Answer:

D

Explanation:

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.