DUMPSARENA

EC-Council Certified Encryption Specialist (ECES)

ECCouncil 212-81

Version Demo

Total Demo Questions: 10

Total Premium Questions: 199

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

You are explaining the details of the AES algorithm to cryptography students. You are discussing the derivation of the round keys from the shared symmetric key. The portion of AES where round keys are derived from the cipher key using Rijndael's key schedule is called what?

A. The key expansion phase

B. The round key phase

C. The bit shifting phase

D. The initial round

ANSWER: A

Explanation:

Explanation

The key expansion phase

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

KeyExpansion – round keys are derived from the cipher key using the AES key schedule. AES requires a separate 128-bit round key block for each round plus one more.

QUESTION NO: 2

If the round function is a cryptographically secure pseudorandom function, then ___rounds is sufficient to make it a "strong" pseudorandom permutation.

A. 15

B. 16

C. 3

D. 4

ANSWER: D

Explanation:

Explanation

4

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 NO: 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

ANSWER: A C

Explanation:

Explanation

K3 and K4

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

The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) has established four criteria for quality of deterministic random number generators.They are summarized here:

K1 – There should be a high probability that generated sequences of random numbers are different from each other.

K2 – A sequence of numbers is indistinguishable from "truly random" numbers according to specified statistical tests. The tests are the monobit test (equal numbers of ones and zeros in the sequence), poker test (a special instance of the chi-squared test), runs test (counts the frequency of runs of various lengths), longruns test (checks whether there exists any run of length 34 or greater in 20 000 bits of the sequence)—both from BSI and NIST, and the autocorrelation test. In essence, these requirements are a test of how well a bit sequence: has zeros and ones equally often; after a sequence of n zeros (or ones), the next bit a one (or zero) with probability one-half; and any selected subsequence contains no information about the next element(s) in the sequence.

K3 – It should be impossible for an attacker (for all practical purposes) to calculate, or otherwise guess, from any given subsequence, any previous or future values in the sequence, nor any inner state of the generator.

K4 – It should be impossible, for all practical purposes, for an attacker to calculate, or guess from an inner state of the generator, any previous numbers in the sequence or any previous inner generator states.

For cryptographic applications, only generators meeting the K3 or K4 standards are acceptable.

QUESTION NO: 4

Uses a formula, M_n = 2^n − 1 where n is a prime number, to generate primes. Works for 2, 3, 5, 7 but fails on 11 and on many other n values.

A. Fibonacci Numbers

B. Co-prime Numbers

C. Even Numbers

D. Mersenne Primes

ANSWER: D

Explanation:

Explanation

Correct answers: Mersenne Primes

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

Mersenne prime is a prime number that is one less than a power of two. That is, it is a prime number of the form M_n = 2^n − 1 for some integer n. They are named after Marin Mersenne, a French Minim friar, who studied them in the early 17th century. If n is a composite number then so is 2^n − 1. Therefore, an equivalent definition of the Mersenne primes is that they are the prime numbers of the form M_p = 2^p − 1 for some prime p.

Incorrect answers:

Even Numbers - A formal definition of an even number is that it is an integer of the form n = 2k, where k is an integer; it can then be shown that an odd number is an integer of the form n = 2k + 1 (or alternately, 2k - 1). It is important to realize that the above definition of parity applies only to integer numbers, hence it cannot be applied to numbers like 1/2 or 4.201. See the section "Higher mathematics" below for some extensions of the notion of parity to a larger class of "numbers" or in other more general settings.

Fibonacci Numbers - commonly denoted F_n, form a sequence, called the Fibonacci sequence, such that each number is the sum of the two preceding ones, starting from 0 and 1.

Co-prime Numbers - two integers a and b are said to be relatively prime, mutually prime, or coprime if the only positive integer (factor) that evenly 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.

QUESTION NO: 5

Which one of the following are characteristics of a hash function? (Choose two)

A. Requires a key

B. One-way

C. Fixed length output

D. Symmetric

E. Fast

ANSWER: B C

Explanation:

Correct answers: One-way, Fixed length output

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

A cryptographic hash function is a mathematical algorithm that maps data of arbitrary size (often called the "message") to a bit array of a fixed size (the "hash value", "hash", or "message digest"). It is a one-way function, that is, a function which is practically infeasible to invert.

Incorrect answers:

Symmetric. Cryptographic algorithms can be categorized into three classes: Hash functions, Symmetric and Asymmetric algorithms. Differences: purpose and main fields of application.

Requires a key. Well, technically, this is the correct answer. But in the hash-function, “key” is input data.

Fast. Fast or slow is a subjective characteristic, there are many different algorithms, and here it is impossible to say this unambiguously like "Symmetric encryption is generally faster than asymmetric encryption."

QUESTION NO: 6

Which of the following is required for a hash?

A. Not vulnerable to a brute force attack

B. Few collisions

C. Must use SALT

D. Not reversible

E. Variable length input, fixed length output

F. Minimum key length

ANSWER: D E

Explanation:

Explanation

Correct answers: Variable length input, fixed length output and Not reversible

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

A hash function is any function that can be used to map data of arbitrary size to fixed-size values. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. The values are used to index a fixed-size table called a hash table. Use of a hash function to index a hash table is called hashing or scatter storage addressing.

QUESTION NO: 7

Which of the following is a substitution cipher used by ancient Hebrew scholars?

A. Atbash

B. Vigenere

C. Caesar

D. Scytale

ANSWER: A

Explanation:

Atbash

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

Atbash is a monoalphabetic substitution cipher originally used to encrypt the Hebrew alphabet. It can be modified for use with any known writing system with a standard collating order.

Incorrect answers:

Scytale - Transposition cipher. A staff with papyrus or letter wrapped around it so edges would line up. There would be a stream of characters which would show you your message. When unwound it would be a random string of characters. Would need an identical size staff on other end for other individuals to decode message.

Vigenère - method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It employs a form of polyalphabetic substitution.

Caesar Cipher - Monoalphabetic cipher where letters are shifted one or more letters in either direction. The method is named after Julius Caesar, who used it in his private correspondence.

QUESTION NO: 8

John is responsible for VPNs at his company. He is using IPSec because it has two different modes. He can choose the mode appropriate for a given situation. What are the two modes of IPSec? (Choose two)

A. Encrypt mode

B. Transport mode

C. Tunnel mode

D. Decrypt mode

ANSWER: B C

Explanation:

Correct answers: Transport mode and Tunnel mode

https://en.wikipedia.org/wiki/IPsec#Modes_of_operation

The IPsec protocols AH and ESP can be implemented in a host-to-host transport mode, as well as in a network tunneling mode.

QUESTION NO: 9

Electromechanical rotor-based cipher used in World War II

A. ROT13 Cipher

B. Cipher Disk

C. Enigma Machine

D. Rail Fence Cipher

ANSWER: C

Explanation:

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.

Incorrect answers:

Rail Fence Cipher - a form of transposition cipher. In the rail fence cipher, the plain text is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when the bottom rail is reached. When the top rail is reached, the message is written downwards again until the whole plaintext is written out. The message is then read off in rows.

Cipher Disk - an enciphering and deciphering tool developed in 1470 by the Italian architect and author Leon Battista Alberti. He constructed a device, (eponymously called the Alberti cipher disk) consisting of two concentric circular plates mounted one on top of the other. The larger plate is called the "stationary" and the smaller one the "moveable" since the smaller one could move on top of the "stationary". The first incarnation of the disk had plates made of copper and featured the alphabet, in order, inscribed on the outer edge of each disk in cells split evenly along the circumference of the circle. This enabled the two alphabets to move relative to each other creating an easy to use key. Rather than using an impractical and complicated table indicating the encryption method, one could use the much simpler cipher disk. This made both encryption and decryption faster, simpler and less prone to error.

ROT13 Cipher - ("rotate by 13 places", sometimes hyphenated ROT-13) is a simple letter substitution cipher that replaces a letter with the 13th letter after it, in the alphabet. ROT13 is a special case of the Caesar cipher which was developed in ancient Rome.

QUESTION NO: 10

Which of the following are valid key sizes for AES (choose three)?

A. 192

B. 56

C. 256

D. 128

E. 512

F. 64

ANSWER: A C D

Explanation:

Correct answers: 128, 192, 256

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

The Advanced Encryption Standard (AES), also known by its original name Rijndael, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.