DUMPSBOSS.

EC-Council Certified Encryption Specialist (ECES)

ECCouncil 212-81

Version Demo

Total Demo Questions: 10

Total Premium Questions: 199

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

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: 2

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

ANSWER: A

Explanation:

Explanation

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.

QUESTION NO: 3

Which one of the following is an authentication method that sends the username and password in cleartext?

A. PAP

B. CHAP

C. Kerberos

D. SPAP

ANSWER: A

Explanation:

PAP

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

Password Authentication Protocol (PAP) is a password-based authentication protocol used by Point to Point Protocol (PPP) to validate users. Almost all network operating system remote servers support PAP. PAP is specified in RFC 1334.

PAP is considered a weak authentication scheme (weak schemes are simple and have lighter computational overhead but are much more vulnerable to attack; while weak schemes may have limited application in some constrained environments, they are avoided in general). Among PAP's deficiencies is the fact that it transmits unencrypted passwords (i.e. in plain-text) over the network. PAP is therefore used only as a last resort when the remote server does not support a stronger scheme such as CHAP or EAP.

Incorrect answers:

SPAP - Shiva Password Authentication Protocol, PAP with encryption for the usernames/passwords that are transmitted.

CHAP - calculates a hash, shares the hash with the client system, the hash is periodically validated to ensure nothing has changed.

Kerberos - computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed it primarily at a client–server model and it provides mutual authentication—both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.

Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication.

QUESTION NO: 4

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: 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

The mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext.

A. Cipher-block chaining (CBC)

B. Electronic codebook (ECB)

C. Output feedback (OFB)

D. Cipher feedback (CFB)

ANSWER: C

Explanation:

Explanation

Output feedback (OFB)

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Output_feedback_(OFB)

The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error-correcting codes to function normally even when applied before encryption.

Incorrect answers:

Cipher feedback (CFB) - mode, a close relative of CBC, makes a block cipher into a self-synchronizing stream cipher.

Electronic codebook (ECB) - the simplest of the encryption modes (named after conventional physical codebooks). The message is divided into blocks, and each block is encrypted separately.

Cipher-block chaining (CBC) - Ehrsam, Meyer, Smith and Tuchman invented the cipher block chaining (CBC) mode of operation in 1976. In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.

QUESTION NO: 7

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.

QUESTION NO: 8

The art and science of writing hidden messages so that no one suspects the existence of the message, a type of security through obscurity. Message can be hidden in picture or audio file for example. Uses least significant bits in a file to store data.

A. Steganography

B. Cryptosystem

C. Avalanche effect

D. Key Schedule

ANSWER: A

Explanation:

Steganography

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

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages appear to be (or to be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some implementations of steganography that lack a shared secret are forms of security through obscurity, and key-dependent steganographic schemes adhere to Kerckhoffs's principle.

Incorrect answers:

Avalanche effect - the desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions, wherein if an input is changed slightly (for example, flipping a single bit), the output changes significantly (e.g., half the output bits flip). In the case of high-quality block ciphers, such a small change in either the key or the plaintext should cause a drastic change in the ciphertext.

Cryptosystem - a suite of cryptographic algorithms needed to implement a particular security service, most commonly for achieving confidentiality (encryption)

Key Schedule - an algorithm for the key that calculates the subkeys for each round that the encryption goes through.

QUESTION NO: 9

Ahlen is using a set of pre-calculated hashes to attempt to derive the passwords from a Windows SAM file. What is a set of pre-calculated hashes used to derive a hashed password called?

A. Hash matrix

B. Rainbow table

C. Password table

D. Hash table

ANSWER: B

Explanation:

Explanation

Rainbow table

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

A rainbow table is a precomputed table for caching the output of cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a key derivation function (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters. It is a practical example of a space–time tradeoff, using less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple key derivation function with one entry per hash. Use of a key derivation that employs a salt makes this attack infeasible.

QUESTION NO: 10

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.