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.leads4pass.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

A cryptanalysis success where the attacker discovers additional plain texts (or cipher texts) not previously known.

A. Total Break

B. Distinguishing Algorithm

C. Instance Deduction

D. Information Deduction

Correct Answer: C

Instance Deduction

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

The results of cryptanalysis can also vary in usefulness. For example, cryptographer Lars Knudsen (1998) classified various types of attack on block ciphers according to the amount and quality of secret information that was discovered:

Total break -- the attacker deduces the secret key. Global deduction -- the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key. Instance (local) deduction -- the attacker discovers

additional plaintexts (or ciphertexts) not previously known.

Information deduction -- the attacker gains some Shannon information about plaintexts (or ciphertexts) not previously known.

Distinguishing algorithm -- the attacker can distinguish the cipher from a random permutation.

QUESTION 2

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

Correct Answer: BC

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 3

Developed by Netscape and has been replaced by TLS. It was the preferred method used with secure websites.

A. OCSP

B. VPN

C. CRL

D. SSL

Correct Answer: D

SSL https://en.wikipedia.org/wiki/Transport_Layer_Security Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. Several versions of the protocols find widespread use in applications such as web browsing, email, instant messaging, and voice over IP (VoIP). Websites can use TLS to secure all communications between their servers and web browsers. Netscape developed the original SSL protocols, and Taher Elgamal, chief scientist at Netscape Communications from 1995 to 1998, has been described as the "father of SSL". SSL version 1.0 was never publicly released because of serious security flaws in the protocol. Version 2.0, released in February 1995, contained a number of security flaws which necessitated the design of version 3.0. Released in 1996, SSL version 3.0 represented a complete redesign of the protocol produced by Paul Kocher working with Netscape engineers Phil Karlton and Alan Freier, with a reference implementation by Christopher Allen and Tim Dierks of Consensus Development.

QUESTION 4

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.

QUESTION 5

What size block does AES work on?

A. 64

B. 128

C. 192

D. 256

Correct Answer: B

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard 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 6

You are trying to find a modern method for security web traffic for use in your company\\'s ecommerce web site. Which one of the following is used to encrypt web pages and uses bilateral authentication?

A. AES

B. SSL

C. TLS

D. 3DES

Correct Answer: C

TLS https://en.wikipedia.org/wiki/Mutual_authentication Mutual authentication or two-way authentication refers to two parties authenticating each other at the same time, being a default mode of authentication in some protocols (IKE, SSH) and optional in others (TLS). By default the TLS protocol only proves the identity of the server to the client using X.509 certificate and the authentication of the client to the server is left to the application layer. TLS also offers client-to-server authentication using client-side

X.509 authentication. As it requires provisioning of the certificates to the clients and involves less user-friendly experience, it\\'s rarely used in end-user applications.

QUESTION 7

What is an IV?

A. Random bits added to a hash

B. The key used for a cryptography algorith

C. A fixed size random stream that is added to a block cipher to increase randomeness

D. The cipher used

Correct Answer: C

A fixed size random stream that is added to a block cipher to increase randomeness https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Initialization_vector_(IV) An initialization vector (IV) or starting variable (SV) is a block of bits that is used by several modes to randomize the encryption and hence to produce distinct ciphertexts even if the same plaintext is encrypted multiple times, without the need for a slower re-keying process.

QUESTION 8

Basic information theory is the basis for modern symmetric ciphers. Understanding the terminology of information theory is, therefore, important. If a single change of a single bit in the plaintext causes changes in all the bits of the resulting ciphertext, what is this called?

A. Complete diffusion

B. Complete scrambling

C. Complete confusion

D. Complete avalanche

Correct Answer: D

QUESTION 9

A symmetric block cipher designed in 1993 by Bruce Schneier. Was intended as a replacement for DES. Like DES it is a 16 round Feistel working on 64bit blocks. Can have bit sizes 32bits to 448bits.

A. Skipjack

B. Blowfish

C. MD5

D. Serpent

Correct Answer: B

Blowfish https://en.wikipedia.org/wiki/Blowfish_(cipher) Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in many cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention, and Schneier recommends Twofish for modern applications. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes.

QUESTION 10

Which of the following is a fundamental principle of cryptography that holds that the algorithm can be publicly disclosed without damaging security?

A. Vigenere\\'s principle

B. Shamir\\'s principle

C. Kerkchoff\\'s principle

D. Babbage\\'s principle

Correct Answer: C

Kerkchoff\\'s principle https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle Kerckhoffs\\'s principle (also called Kerckhoffs\\'s desideratum, assumption, axiom, doctrine or law) of cryptography was stated by Netherlands born cryptographer Auguste Kerckhoffs in the 19th century: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge. Kerckhoffs\\'s principle was reformulated (or possibly independently formulated) by American mathematician Claude Shannon as "the enemy knows the system", i.e., "one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them". In that form, it is called Shannon\\'s maxim. This concept is widely embraced by cryptographers, in contrast to "security through obscurity", which is not.

QUESTION 11

Which of the following is an asymmetric cipher?

A. RSA

B. AES

C. DES

D. RC4

Correct Answer: A

RSA

https://en.wikipedia.org/wiki/RSA_(cryptosystem)

RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who

publicly described the algorithm in 1977. An equivalent system was developed secretly, in 1973 at GCHQ (the British signals intelligence agency), by the English mathematician Clifford Cocks. That system was declassified in 1997.

In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value.

The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

QUESTION 12

A 160-bit hash algorithm developed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel for which there are 128, 256 and 320-bit versions is called what?

A. SHA1

B. MD5

C. FORK

D. RIPEMD

Correct Answer: D

RIPEMD https://en.wikipedia.org/wiki/RIPEMD RIPEMD (RIPE Message Digest) is a family of cryptographic hash functions developed in 1992 (the original RIPEMD) and 1996 (other variants). There are five functions in the family: RIPEMD, RIPEMD-128, RIPEMD-160, RIPEMD-256, and RIPEMD-320, of which RIPEMD-160 is the most common. The original RIPEMD, as well as RIPEMD-128, is not considered secure because 128-bit result is too small and also (for the original RIPEMD) because of design weaknesses. The 256- and 320-bit versions of RIPEMD provide the same level of security as RIPEMD-128 and RIPEMD-160, respectively; they are designed for applications where the security level is sufficient but longer hash result is necessary.

QUESTION 13

A non-secret binary vector used as the initializing input algorithm for encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance.

A. IV

B. Salt

C. L2TP

D. Nonce

Correct Answer: A

IV https://en.wikipedia.org/wiki/Initialization_vector In cryptography, an initialization vector (IV) or starting variable (SV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. For block ciphers, the use of an IV is described by the modes of operation. Randomization is also required for other primitives, such as universal hash functions and message authentication codes based thereon.

QUESTION 14

Which of the following is used to encrypt email and create digital signatures?

A. DES

B. SHA1

C. AES

D. RSA

Correct Answer: D

RSA https://en.wikipedia.org/wiki/RSA_(cryptosystem) RSA use for encryption email and create digital signatures

QUESTION 15

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

A. Atbash

B. Vigenere

C. Caesar

D. Scytale

Correct Answer: A

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.