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.certbus.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

What type of encryption uses different keys to encrypt and decrypt the message?

A. Asymmetric

B. Symmetric

C. Secure

D. Private key

Correct Answer: A

Asymmetric https://en.wikipedia.org/wiki/Public-key_cryptography 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.

QUESTION 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

Correct Answer: D

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 3

Which of the following is a type of encryption that has two different keys. One key can encrypt the message and the other key can only decrypt it?

A. Block cipher

B. Asymmetric

C. Symmetric

D. Stream cipher

Correct Answer: B

Asymmetric 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.

QUESTION 4

A transposition cipher invented 1918 by Fritz Nebel, used a 36 letter alphabet and a modified Polybius square with a single columnar transposition.

A. ADFVGX Cipher

B. ROT13 Cipher

C. Book Ciphers

D. Cipher Disk

Correct Answer: A

ADFVGX Cipher https://en.wikipedia.org/wiki/ADFGVX_cipher ADFGVX cipher was a field cipher used by the German Army on the Western Front during World War I. ADFGVX was in fact an extension of an earlier cipher called ADFGX. Invented by Lieutenant Fritz Nebel (1891?977) and introduced in March 1918, the cipher was a fractionating transposition cipher which combined a modified Polybius square with a single columnar transposition.

QUESTION 5

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 6

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

Correct Answer: BC

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.

QUESTION 7

Which of the following is a block cipher?

A. AES

B. DH

C. RC4

D. RSA

Correct Answer: A

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

QUESTION 8

Which of the following is an asymmetric algorithm related to the equation y^2 = x^3 + Ax + B?

A. Blowfish

B. Elliptic Curve

C. AES

D. RSA

Correct Answer: B

Elliptic Curve

https://en.wikipedia.org/wiki/Elliptic-curve_cryptography For current cryptographic purposes, an elliptic curve is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation:

QUESTION 9

Which of the following is a cryptographic protocol that allows two parties to establish a shared key over an insecure channel?

A. Elliptic Curve

B. NMD5

C. RSA

D. Diffie-Hellman

Correct Answer: D

Diffie-Hellman https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange Diffie-Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography.

QUESTION 10

Software for maintaining an on-the-fly-encrypted volume. Data is automatically encrypted right before it is saved, then decrypted right after it is loaded, all w/o user intervention.

A. VPN

B. PGP

C. Cryptool

D. VeraCrypt

Correct Answer: D

VeraCrypt https://en.wikipedia.org/wiki/VeraCrypt VeraCrypt is a source-available freeware utility used for on-the-fly encryption (OTFE). It can create a virtual encrypted disk within a file or encrypt a partition or (in Windows) the entire storage device with pre-boot authentication.

QUESTION 11

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 12

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

A. Coprime

B. Fermat\\'s number

C. Euler\\'s totient

D. Convergent

Correct Answer: A

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.

QUESTION 13

Changes to one character in the plain text affect multiple characters in the cipher text, unlike in historical algorithms where each plain text character only affect one cipher text character.

A. Substitution

B. Avalanche

C. Confusion

D. Diffusion

Correct Answer: D

Diffusion https://en.wikipedia.org/wiki/Confusion_and_diffusion Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change.[2] Since a bit can have only two states, when they are all re-evaluated and changed from one seemingly random position to another, half of the bits will have changed state. The idea of diffusion is to hide the relationship between the ciphertext and the plain text. This will make it hard for an attacker who tries to find out the plain text and it increases the redundancy of plain text by spreading it across the rows and columns; it is achieved through transposition of algorithm and it is used by block ciphers only.

QUESTION 14

Ciphers that write message letters out diagonally over a number of rows then read off cipher row by row. Also called zig-zag cipher.

A. Rail Fence Cipher

B. Null Cipher

C. Vigenere Cipher

D. ROT-13

Correct Answer: A

Rail Fence Cipher https://en.wikipedia.org/wiki/Rail_fence_cipher The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded.

QUESTION 15

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.