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.pass2lead.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

Bruce Schneier is a well-known and highly respected cryptographer. He has developed several pseudo random number generators as well as worked on teams developing symmetric ciphers. Which one of the following is a symmetric block cipher designed in 1993 by Bruce Schneier team that is unpatented?

A. Pegasus

B. Blowfish

C. SHA1

D. AES

Correct Answer: A

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.

QUESTION 2

A _____ product refers to an NSA-endorsed classified or controlled cryptographic item for classified or sensitive U. S. government information, including cryptographic equipment, assembly, or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed

A. 1

B. 4

C. 2

D. 3

Correct Answer: A

Type 1 https://en.wikipedia.org/wiki/NSA_cryptography#Type_1_Product A Type 1 Product refers to an NSA endorsed classified or controlled cryptographic item for classified or sensitive U.S. government information, including cryptographic equipment, assembly or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed.

QUESTION 3

Juanita is attempting to hide some text into a jpeg file. Hiding messages inside another medium is referred to as which one of the following?

A. Cryptography

B. Steganalysis

C. Cryptology

D. Steganography

Correct Answer: D

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

QUESTION 4

The time and effort required to break a security measure.

A. Session Key

B. Work factor

C. Non-repudiation

D. Payload

Correct Answer: B

Work factor

Work factor - the time and effort required to break a security measure.

QUESTION 5

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

Correct Answer: B

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 6

John is going to use RSA to encrypt a message to Joan. What key should he use?

A. A random key

B. Joan\\'s public key

C. A shared key

D. Joan\\'s private key

Correct Answer: B

Joan\\'s public key https://en.wikipedia.org/wiki/RSA_(cryptosystem) Suppose Joahn uses Bob\\'s public key to send him an encrypted message. In the message, she can claim to be Alice but Bob has no way of verifying that the message was actually from Alice since anyone can use Bob\\'s public key to send him encrypted messages. In order to verify the origin of a message, RSA can also be used to sign a message. Suppose Alice wishes to send a signed message to Bob. She can use her own private key to do so. She produces a hash value of the message, raises it to the power of d (modulo n) (as she does when decrypting a message), and attaches it as a "signature" to the message. When Bob receives the signed message, he uses the same hash algorithm in conjunction with Alice\\'s public key. He raises the signature to the power of e (modulo n) (as he does when encrypting a message), and compares the resulting hash value with the message\\'s actual hash value. If the two agree, he knows that the author of the message was in possession of Alice\\'s private key, and that the message has not been tampered with since.

QUESTION 7

Which of the following are required for a hash? (Choose two)

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

Correct Answer: DE

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 8

This is a proprietary version of PAP. Encrypts username and password as it is sent across network.

A. PPTP VPN

B. S-PAP

C. Kerberos

D. WPA2

Correct Answer: B

S-PAP

Shiva Password Authentication Protocol (S-PAP) - PAP with encryption for the usernames/passwords that are transmitted.

QUESTION 9

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.

A. Lehmer Random Number Generator

B. Lagged Fibonacci Generator

C. Linear Congruential Generator

D. Blum Blum Shub

Correct Answer: A

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?iller 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 10

Which of the following is the standard for digital certificates?

A. RFC 2298

B. X.509

C. CRL

D. CA

Correct Answer: B

https://en.wikipedia.org/wiki/X.509

X.509 is a standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web. They are also used in offline applications, like electronic signatures. An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.

QUESTION 11

An attack that is particularly successful against block ciphers based on substitution- permutation networks. For a block size b, holds b-k bits constant and runs the other k through all 2k possibilities. For k=1, this is just deferential cryptanalysis, but with k>1 it is a new technique.

A. Differential Cryptanalysis

B. Linear Cryptanalysis

C. Chosen Plaintext Attack

D. Integral Cryptanalysis

Correct Answer: D

Integral Cryptanalysis https://en.wikipedia.org/wiki/Integral_cryptanalysis Integral cryptanalysis is a cryptanalytic attack that is particularly applicable to block ciphers based on substitution-permutation networks. It was originally designed by Lars Knudsen as a dedicated attack against Square, so it is commonly known as the Square attack. It was also extended to a few other ciphers related to Square: CRYPTON, Rijndael, and SHARK. Stefan Lucks generalized the attack to what he called a saturation attack and used it to attack Twofish, which is not at all similar to Square, having a radically different Feistel network structure. Forms of integral cryptanalysis have since been applied to a variety of ciphers, including Hierocrypt, IDEA, Camellia, Skipjack, MISTY1, MISTY2, SAFER++, KHAZAD, and FOX (now called IDEA NXT).

QUESTION 12

Hash. Created by Ronald Rivest. Replaced MD4. 128 bit output size, 512 bit block size, 32 bit word size, 64 rounds. Infamously compromised by Flame malware in 2012.

A. Keccak

B. MD5

C. SHA-1

D. TIGER

Correct Answer: B

MD5 https://en.wikipedia.org/wiki/MD5 The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against

unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database. MD5 was designed by Ronald Rivest in 1991 to replace an earlier hash function MD4, and was specified in 1992 as RFC 1321

QUESTION 13

Which of the following equations is related to EC?

A. P = Cd%n

B. Me%n

C. y^2 = x^3 + Ax + B

D. Let m = (p-1)(q-1)

Correct Answer: C

y^2 = x^3 + Ax + B

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 14

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 15

Cylinder tool. Wrap leather around to decode. The diameter is the key. Used in 7th century BC by greek poet Archilochus.

A. Cipher disk

B. Caesar cipher

C. Scytale

D. Enigma machine

Correct Answer: C

Scytale https://en.wikipedia.org/wiki/Scytale A scytale is a tool used to perform a transposition cipher, consisting of a cylinder with a strip of parchment wound around it on which is written a message. The ancient Greeks, and the Spartans in particular, are said to have used this cipher in 7th century BC to communicate during military campaigns. The recipient uses a rod of the same diameter on which the parchment is wrapped to read the message. It has the advantage of being fast and not prone to mistakes--a necessary property when on the battlefield. It can, however, be easily broken. Since the strip of parchment hints strongly at the method, the ciphertext would have to be transferred to something less suggestive, somewhat reducing the advantage noted.