212-81$^{\text{Q\&As}}$

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.pass4itsure.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 _____ is a function is not reversible.

A. Stream cipher

B. Asymmetric cipher

C. Hash

D. Block Cipher

Correct Answer: C

Hash https://en.wikipedia.org/wiki/Hash_function Hash functions are irreversible. This is actually required for them to fulfill their function of determining whether someone possesses an uncorrupted copy of the hashed data. This brings susceptibility to brute force attacks, which are quite powerful these days, particularly against MD5.

QUESTION 2

Which of the following is a protocol for exchanging keys?

A. DH

B. EC

C. AES

D. RSA

Correct Answer: A

DH 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 conceived 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. Published in 1976 by Diffie and Hellman, this is the earliest publicly known work that proposed the idea of a private key and a corresponding public key.

QUESTION 3

Which of the following acts as a verifier for the certificate authority?

A. Certificate Management system

B. Directory management system

C. Registration authority

D. Certificate authority

Correct Answer: C

Registration authority https://en.wikipedia.org/wiki/Registration_authority Registration authorities exist for many standards organizations, such as ANNA (Association of National Numbering Agencies for ISIN), the Object Management Group, W3C, IEEE and others. In general, registration authorities all perform a similar function, in promoting the use of a particular standard through facilitating its use. This may be by applying the standard, where appropriate, or by verifying that a particular application satisfies the standard\\'s tenants. Maintenance agencies, in contrast, may change an element in a standard based on set rules ?such as the creation or change of a currency code when a currency is created or revalued (i.e. TRL to TRY for Turkish lira). The Object Management Group has an additional concept of certified provider, which is deemed an entity permitted to perform some functions on behalf of the registration authority, under specific processes and procedures documented within the standard for such a role.

QUESTION 4

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 5

If the round function is a cryptographically secure pseudorandom function, then ___________ rounds is sufficient to make the block cipher a pseudorandom permutation.

A. 2

B. 15

C. 16

D. 3

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 6

As a network administrator, you have implemented WPA2 encryption in your corporate wireless network. The WPA2\\'s ________ integrity check mechanism provides security against a replay attack.

A. CBC-MAC

B. CRC-MAC

C. CRC-32

D. CBC-32

Correct Answer: A

CBC-MAC https://en.wikipedia.org/wiki/CBC-MAC A cipher block chaining message authentication code (CBC-MAC) is a technique for constructing a message authentication code from a block cipher. The message is encrypted with some block cipher algorithm in CBC mode to create a chain of blocks such that each block depends on the proper encryption of the previous block. This interdependence ensures that a change to any of the plaintext bits will cause the final encrypted block to change in a way that cannot be predicted or counteracted without knowing the key to the block cipher. Using in WPA2 for integrity check and provides security against a replay attack.

QUESTION 7

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 8

The concept that if one bit of data changes, the cipher text will all completely change as well.

A. Avalanche

B. Substitution

C. Confusion

D. Collision

Correct Answer: A

Avalanche https://en.wikipedia.org/wiki/Avalanche_effect In cryptography, the avalanche effect is 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. The actual term was first used by Horst Feistel, although the concept dates back to at least Shannon\\'s diffusion.

QUESTION 9

Hash algortihm created by the Russians. Produces a fixed length output of 256bits. Input message is broken up into 256 bit blocks. If block is less than 256 bits then it is padded with 0s.

A. TIGER

B. GOST

C. BEAR

D. FORK-256

Correct Answer: B

GOST https://en.wikipedia.org/wiki/GOST_(hash_function) The GOST hash function, defined in the standards GOST R 34.11-94 and GOST 34.311- 95 is a 256-bit cryptographic hash function. It was initially defined in the Russian national standard GOST R 34.11-94 Information Technology ?Cryptographic Information Security ?Hash Function. The equivalent standard used by other member-states of the CIS is GOST 34.311-95.

QUESTION 10

Represents the total number of possible values of keys in a cryptographic algorithm or other security measure, such as a password.

A. Key Schedule

B. Key Clustering

C. Key Space

D. Key Exchange

Correct Answer: C

Key Space https://en.wikipedia.org/wiki/Key_space_(cryptography) Algorithm\\'s key space refers to the set of all possible permutations of a key. To prevent an adversary from using a brute-force attack to find the key used to encrypt a message, the key space is usually designed to be large enough to make such a search infeasible. On average, half the key space must be searched to find the solution. Another desirable attribute is that the key must be selected truly randomly from all possible key permutations. Should this not be the case, and the attacker is able to determine some factor that may influence how the key was selected, the search space (and hence also the search time) can be significantly reduced. Humans do not select passwords randomly, therefore attackers frequently try a dictionary attack before a brute force attack, as this approach can often produce the correct answer in far less time than a systematic brute force search of all possible character combinations.

QUESTION 11

A digital document that contains a public key and some information to allow your system to verify where that key came from. Used for web servers, Cisco Secure phones, E- Commerce.

A. Registration Authority

B. Payload

C. OCSP

D. Digital Certificate

Correct Answer: D

Digital Certificate https://en.wikipedia.org/wiki/Public_key_certificate A public key certificate, also known as a digital certificate or identity certificate, is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate\\'s contents (called the issuer).

QUESTION 12

In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known as wardriving.

Which Algorithm is this referring to?

A. Wired Equivalent Privacy (WEP)

B. Wi-Fi Protected Access 2 (WPA2)

C. Wi-Fi Protected Access (WPA)

D. Temporal Key Integrity Protocol (TKIP)

Correct Answer: A

Wired Equivalent Privacy (WEP) https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy#Weak_security In 2007, Erik Tews, Andrei Pychkine, and Ralf-Philipp Weinmann were able to extend Klein\\'s 2005 attack and optimize it for usage against WEP. With the new attack it is possible to recover a 104-bit WEP key with probability 50% using only 40,000 captured packets. For 60,000 available data packets, the success probability is about 80% and for 85,000 data packets about 95%. Using active techniques like deauth and ARP re-injection, 40,000 packets can be captured in less than one minute under good conditions. The actual computation takes about 3 seconds and 3 MB of main memory on a Pentium-M 1.7 GHz and can additionally be optimized for devices with slower CPUs. The same attack can be used for 40-bit keys with an even higher success probability.

QUESTION 13

Basic information theory is the basis for modern symmetric ciphers. Understanding the terminology of information theory is, therefore, important. Changes to one character in the plaintext affect multiple characters in the ciphertext. What is this referred to?

A. Avalanche

B. Confusion

C. Scrambling

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. 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

The greatest weakness with symmetric algorithms is _____.

A. They are less secure than asymmetric

B. The problem of key exchange

C. The problem of generating keys

D. They are slower than asymmetric

Correct Answer: B

The problem of key exchange https://en.wikipedia.org/wiki/Symmetric-key_algorithm Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption (also known as asymmetric key encryption).

QUESTION 15

A real time protocol for verifying certificates (and a newer method than CRL).

A. Online Certificate Status Protocol (OCSP)

B. Server-based Certificate Validation Protocol (SCVP)

C. Public Key Infrastructure (PKI)

D. Registration Authority (RA)

Correct Answer: A

Online Certificate Status Protocol (OCSP)

https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 6960 and is on

the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI).