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.passapply.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

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)

Correct Answer: C

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.

QUESTION 2

Which service in a PKI will vouch for the identity of an individual or company?

A. CA

B. CR

C. KDC

D. CBC

Correct Answer: A

CA

https://en.wikipedia.org/wiki/Certificate_authority A certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.

This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party--trusted both by the subject (owner) of the certificate and by

the party relying upon the certificate. The format of these certificates is specified by the X.509 or EMV standard.

QUESTION 3

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 4

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 5

Jane is looking for an algorithm to ensure message integrity. Which of following would be an acceptable choice?

A. RSA

B. AES

C. RC4

D. SHA-1

Correct Answer: D

Integrity. In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner. An important application of hashes is verification of message integrity. Comparing message digests (hash digests over the message) calculated before, and after, transmission can determine whether any changes have been made to the message or file. SHA-1 https://en.wikipedia.org/wiki/SHA-1 SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest ?typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard.