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.geekcert.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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which one of the following is an example of a symmetric key algorithm?

A. ECC

B. Diffie-Hellman

C. RSA

D. Rijndael

Correct Answer: D

Rijndael https://en.wikipedia.org/wiki/Advanced_Encryption_Standard The Advanced Encryption Standard (AES), also known by its original name Rijndael. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

QUESTION 2

Which of the following would be the fastest.

A. EC

B. DH

C. RSA

D. AES

Correct Answer: D

AES https://en.wikipedia.org/wiki/Symmetric-key_algorithm AES - symmetric cipher. Symmetric keys use the same key for both encryption and decryption. Both the sender and receiver of the data must know and share the secret key. For standard encrypt/decrypt functions, symmetric algorithms generally perform much faster than their asymmetrical counterparts. This is due to the fact that asymmetric cryptography is massively inefficient. Symmetric cryptography is designed precisely for the efficient processing of large volumes of data. In other words, symmetric encryption is generally used for speed and performance, e.g. when there\\'s a large amount of data that needs to be encrypted/protected.

QUESTION 3

A number that is used only one time, then discarded is called what?

A. IV

B. Nonce

C. Chain

D. Salt

Correct Answer: B

Nonce https://en.wikipedia.org/wiki/Cryptographic_nonce A nonce is an arbitrary number that can be used just once in a cryptographic communication. It is similar in spirit to a nonce word, hence the name. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks.

QUESTION 4

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 5

If you XOR 10111000 with 10101010, what is the result?

A. 10111010

B. 10101010

C. 11101101

D. 00010010

Correct Answer: D

https://en.wikipedia.org/wiki/XOR_cipher 1 0 1 1 1 0 0 0 1 0 1 0 1 0 1 0

0 0 0 1 0 0 1 0