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 ATBASH cipher is best described as what type of cipher?

A. Asymmetric

B. Symmetric

C. Substitution D. Transposition

Correct Answer: C

Substitution https://en.wikipedia.org/wiki/Atbash Atbash is a monoalphabetic substitution cipher originally used to encrypt the Hebrew alphabet. It can be modified for use with any known writing system with a standard collating order.

QUESTION 2

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 3

What size block does Skipjack use?

A. 64

B. 512

C. 128

D. 256

Correct Answer: A

https://en.wikipedia.org/wiki/Skipjack_(cipher)

Skipjack uses an 80-bit key to encrypt or decrypt 64-bit data blocks. It is an unbalanced Feistel network with 32 rounds.

QUESTION 4

Developed by Netscape and has been replaced by TLS. It was the preferred method used with secure websites.

A. OCSP

B. VPN

C. CRL

D. SSL

Correct Answer: D

SSL https://en.wikipedia.org/wiki/Transport_Layer_Security Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. Several versions of the protocols find widespread use in applications such as web browsing, email, instant messaging, and voice over IP (VoIP). Websites can use TLS to secure all communications between their servers and web browsers. Netscape developed the original SSL protocols, and Taher Elgamal, chief scientist at Netscape Communications from 1995 to 1998, has been described as the "father of SSL". SSL version 1.0 was never publicly released because of serious security flaws in the protocol. Version 2.0, released in February 1995, contained a number of security flaws which necessitated the design of version 3.0. Released in 1996, SSL version 3.0 represented a complete redesign of the protocol produced by Paul Kocher working with Netscape engineers Phil Karlton and Alan Freier, with a reference implementation by Christopher Allen and Tim Dierks of Consensus Development.

QUESTION 5

With Cipher feedback (CFB) what happens?

A. The key is reapplied

B. The ciphertext block is encrypted then the ciphertext produced is XOR\\'d back with the plaintext to produce the current ciphertext block

C. The block cipher is turned into a stream cipher

D. The message is divided into blocks and each block is encrypted separately. This is the most basic mode for symmetric encryption

Correct Answer: B

The ciphertext block is encrypted then the ciphertext produced is XOR\\'d back with the plaintext to produce the current ciphertext block https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Cipher_feedback_(CFB) The cipher feedback (CFB) mode, a close relative of CBC, makes a block cipher into a self- synchronizing stream cipher.