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

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 2

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 3

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 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

With Cipher-block chaining (CBC) what happens?

A. The block cipher is turned into a stream cipher

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

C. Each block of plaintext is XORed with the previous ciphertext block before being encrypted

D. The cipher text from the current round is XORed with the plaintext for the next round

Correct Answer: C

Each block of plaintext is XORed with the previous ciphertext block before being encrypted
https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Cipher_block_chaining_(CB C)

In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an

initialization vector must be used in the first block.