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.pass2lead.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

Changes to one character in the plain text affect multiple characters in the cipher text, unlike in historical algorithms where each plain text character only affect one cipher text character.

A. Substitution

B. Avalanche

C. Confusion

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.[2] 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

Juanita has been assigned the task of selecting email encryption for the staff of the insurance company she works for. The various employees often use diverse email clients. Which of the following methods is available as an add-in for most email clients?

A. Caesar cipher

B. RSA

C. PGP

D. DES

Correct Answer: C

PGP https://en.wikipedia.org/wiki/Pretty_Good_Privacy Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. Phil Zimmermann developed PGP in 1991.

QUESTION 3

Widely used, particularly with Microsoft operating systems. Created by MIT and derives its name from the mythical three headed dog. The is a great deal of verification for the tickets and the tickets expire quickly. Client authenticates to the Authentication Server once using a long term shared secret and receives back a Ticket-Granting Server. Client can reuse this ticket to get additional tickets without reusing the shared secret. These tickets are used to prove authentication to the Service Server.

A. Diffie-Hellman

B. Yarrow

C. Kerberos

D. ElGamal

Correct Answer: C

Kerberos https://en.wikipedia.org/wiki/Kerberos_(protocol) Kerberos is a computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. The protocol was named after the character Kerberos (or Cerberus) from Greek mythology, the ferocious three-headed guard dog of Hades. Its designers aimed it primarily at a client-server model and it provides mutual authentication--both the user and the server verify each other\\'s identity. Kerberos protocol messages are protected against eavesdropping and replay attacks. Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication. Kerberos uses UDP port 88 by default.

QUESTION 4

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 5

What advantage do symmetric algorithms have over asymmetric algorithms

A. It is easier to implement them in software

B. They are more secure

C. They are faster

D. It is easier to exchange keys

Correct Answer: C

They are faster

Symmetric key encryption is much faster than asymmetric key encryption, because both the sender and the recipient of a message to use the same secret key.