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 of the following is a substitution cipher used by ancient Hebrew scholars?

A. Atbash

B. Vigenere

C. Caesar

D. Scytale

Correct Answer: A

Atbash 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 asymmetric algorithms is described by U.S. Patent 5,231,668 and FIPS 186?

A. AES

B. RC4

C. DSA

D. RSA

Correct Answer: C

DSA https://ru.wikipedia.org/wiki/DSA The National Institute of Standards and Technology (NIST) proposed DSA for use in their Digital Signature Standard (DSS) in 1991, and adopted it as FIPS 186 in 1994. DSA is covered by U.S. Patent 5,231,668 , filed July 26, 1991 and now expired, and attributed to David W. Kravitz, a former NSA employee.

QUESTION 3

Which of the following is a cryptographic protocol that allows two parties to establish a shared key over an insecure channel?

A. Elliptic Curve

B. NMD5

C. RSA

D. Diffie-Hellman

Correct Answer: D

Diffie-Hellman https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange Diffie-Hellman key exchange is a

method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography.

QUESTION 4

An attack that is particularly successful against block ciphers based on substitution- permutation networks. For a block size b, holds b-k bits constant and runs the other k through all 2k possibilities. For k=1, this is just deferential cryptanalysis, but with k>1 it is a new technique.

A. Differential Cryptanalysis

B. Linear Cryptanalysis

C. Chosen Plaintext Attack

D. Integral Cryptanalysis

Correct Answer: D

Integral Cryptanalysis https://en.wikipedia.org/wiki/Integral_cryptanalysis Integral cryptanalysis is a cryptanalytic attack that is particularly applicable to block ciphers based on substitution-permutation networks. It was originally designed by Lars Knudsen as a dedicated attack against Square, so it is commonly known as the Square attack. It was also extended to a few other ciphers related to Square: CRYPTON, Rijndael, and SHARK. Stefan Lucks generalized the attack to what he called a saturation attack and used it to attack Twofish, which is not at all similar to Square, having a radically different Feistel network structure. Forms of integral cryptanalysis have since been applied to a variety of ciphers, including Hierocrypt, IDEA, Camellia, Skipjack, MISTY1, MISTY2, SAFER++, KHAZAD, and FOX (now called IDEA NXT).

QUESTION 5

A disk you rotated to encrypt/decrypt. Created by Leon Alberti. Similar technologies were used in the Enigma machine. Considered the forefather of modern encryption.

A. Chi Square

B. Enigma Machine

C. Cipher Disks

D. Scytale Cipher

Correct Answer: C

Cipher disks https://en.wikipedia.org/wiki/Cipher_disk A cipher disk is an enciphering and deciphering tool developed in 1470 by the Italian architect and author Leon Battista Alberti. He constructed a device, (eponymously called the Alberti cipher disk) consisting of two concentric circular plates mounted one on top of the other. The larger plate is called the "stationary" and the smaller one the "moveable" since the smaller one could move on top of the "stationary".