212-81$^{\text{Q\&As}}$

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.leads4pass.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

You are explaining the details of the AES algorithm to cryptography students. You are discussing the derivation of the round keys from the shared symmetric key. The portion of AES where round keys are derived from the cipher key using Rijndael\\'s key schedule is called what?

A. The key expansion phase

B. The round key phase

C. The bit shifting phase

D. The initial round

Correct Answer: A

The key expansion phase

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard KeyExpansion ?round keys are derived from the cipher key using the AES key schedule. AES requires a separate 128-bit round key block for each round plus one more.

QUESTION 2

Which of the following is an asymmetric algorithm that was first publically described in 1977?

A. Elliptic Curve

B. Twofish

C. DESX

D. RSA

Correct Answer: D

RSA

https://en.wikipedia.org/wiki/RSA_(cryptosystem)

RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who

publicly described the algorithm in 1977.

QUESTION 3

Which of the following was a multi alphabet cipher widely used from the 16th century to the early 20th century?

A. Atbash

B. Caesar

C. Scytale

D. Vigenere

Correct Answer: D

QUESTION 4

The Clipper chip is notable in the history of cryptography for many reasons. First, it was designed for civilian used secure phones. Secondly, it was designed to use a very specific symmetric cipher. Which one of the following was originally designed to provide built-in cryptography for the Clipper chip?

A. Blowfish

B. Twofish

C. Skipjack

D. Serpent

Correct Answer: C

Skipjack https://en.wikipedia.org/wiki/Clipper_chip The Clipper chip was a chipset that was developed and promoted by the United States National Security Agency (NSA) as an encryption device that secured "voice and data messages" with a built-in backdoor that was intended to "allow Federal, State, and local law enforcement officials the ability to decode intercepted voice and data transmissions.". It was intended to be adopted by telecommunications companies for voice transmission. Introduced in 1993, it was entirely defunct by 1996. he Clipper chip used a data encryption algorithm called Skipjack to transmit information and the Diffie-Hellman key exchange-algorithm to distribute the cryptokeys between the peers. Skipjack was invented by the National Security Agency of the U.S. Government; this algorithm was initially classified SECRET, which prevented it from being subjected to peer review from the encryption research community. The government did state that it used an 80-bit key, that the algorithm was symmetric, and that it was similar to the DES algorithm. The Skipjack algorithm was declassified and published by the NSA on June 24, 1998. The initial cost of the chips was said to be $16 (unprogrammed) or $26 (programmed), with its logic designed by Mykotronx, and fabricated by VLSI Technology, Inc (see the VLSI logo on the image on this page).

QUESTION 5

A method for cracking modern cryptography. The attacker obtains the cipher texts corresponding to a set of plain texts of own choosing. Allows the attacker to attempt to derive the key. Difficult but not impossible.

A. Chosen Plaintext Attack

B. Steganography

C. Rainbow Tables

D. Transposition

Correct Answer: A

Chosen Plaintext Attack https://en.wikipedia.org/wiki/Chosen-plaintext_attack A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker can obtain the ciphertexts for arbitrary plaintexts. The goal of the attack is to gain information that reduces the security of the encryption scheme.