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

EC-Council Certified Encryption Specialist (ECES)

Pass EC-COUNCIL 212-81 Exam with 100% Guarantee

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

What is an IV?

A. Random bits added to a hash

B. The key used for a cryptography algorith

C. A fixed size random stream that is added to a block cipher to increase randomeness

D. The cipher used

Correct Answer: C

A fixed size random stream that is added to a block cipher to increase randomeness https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Initialization_vector_(IV) An initialization vector (IV) or starting variable (SV) is a block of bits that is used by several modes to randomize the encryption and hence to produce distinct ciphertexts even if the same plaintext is encrypted multiple times, without the need for a slower re-keying process.

QUESTION 2

John is responsible for VPNs at his company. He is using IPSec because it has two different modes. He can choose the mode appropriate for a given situation. What are the two modes of IPSec? (Choose two)

A. Encrypt mode

B. Transport mode

C. Tunnel mode

D. Decrypt mode

Correct Answer: BC

Correct answers: Transport mode and Tunnel mode

https://en.wikipedia.org/wiki/IPsec#Modes_of_operation The IPsec protocols AH and ESP can be implemented in a host-to-host transport mode, as well as in a network tunneling mode.

QUESTION 3

Which algorithm was U. S. Patent 5,231,668, filed on july 26, 1991, attributed to David W. Kravitz, and adopted by the U. S. government in 1993 with FIPS 186?

A. DSA

B. AES

C. RC4

D. RSA

Correct Answer: A

DSA https://en.wikipedia.org/wiki/Digital_Signature_Algorithm 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. This patent was given to "The United States of America as represented by the Secretary of Commerce, Washington, D.C.", and NIST has made this patent available worldwide royalty-free. Claus P. Schnorr claims that his U.S. Patent 4,995,082 (also now expired) covered DSA; this claim is disputed.

QUESTION 4

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 5

A 160-bit hash algorithm developed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel for which there are 128, 256 and 320-bit versions is called what?

A. SHA1

B. MD5

C. FORK

D. RIPEMD

Correct Answer: D

RIPEMD https://en.wikipedia.org/wiki/RIPEMD RIPEMD (RIPE Message Digest) is a family of cryptographic hash functions developed in 1992 (the original RIPEMD) and 1996 (other variants). There are five functions in the family: RIPEMD, RIPEMD-128, RIPEMD-160, RIPEMD-256, and RIPEMD-320, of which RIPEMD-160 is the most common. The original RIPEMD, as well as RIPEMD-128, is not considered secure because 128-bit result is too small and also (for the original RIPEMD) because of design weaknesses. The 256- and 320-bit versions of RIPEMD provide the same level of security as RIPEMD-128 and RIPEMD-160, respectively; they are designed for applications where the security level is sufficient but longer hash result is necessary.

Latest 212-81 Dumps 212-81 PDF Dumps 212-81 Practice Test