EC-Council

Exam Questions 212-81

EC-Council Certified Encryption Specialist (ECES)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
This hash function uses 512-bit blocks and implements preset constants that change after each repetition. Each block is hashed into a 256-bit block through four branches that divides each 512 block into sixteen 32-bit words that are further encrypted and rearranged.

A. SHA-256
B. FORK-256
C. SHA-1
D. RSA

Answer: B

NEW QUESTION 2
A part of understanding symmetric cryptography understands the modes in which it can be used. You are explaining those modes to a group of cryptography students. The most basic encryption mode is _____ .
The message is divided into blocks, and each block is encrypted separately with no modification to the process.

A. Cipher block chaining (CBC)
B. Cipher feedback (CFB)
C. Output feedback (OFB)
D. Electronic codebook (ECB)

Answer: D

NEW QUESTION 3
The greatest weakness with symmetric algorithms is _____.

A. They are less secure than asymmetric
B. The problem of key exchange
C. The problem of generating keys
D. They are slower than asymmetric

Answer: B

NEW QUESTION 4
A _____ refers to a situation where two different inputs yield the same output.

A. Convergence
B. Collision
C. Transposition
D. Substitution

Answer: B

NEW QUESTION 5
The reverse process from encoding - converting the encoded message back into its plaintext format.

A. Substitution
B. Whitening
C. Encoding
D. Decoding

Answer: D

NEW QUESTION 6
If you wished to see a list of revoked certificates from a CA, where would you look?

A. RA
B. RFC
C. CRL
D. CA

Answer: C

NEW QUESTION 7
Which of the following is a substitution cipher used by ancient Hebrew scholars?

A. Atbash
B. Vigenere
C. Caesar
D. Scytale

Answer: A

NEW QUESTION 8
Which of the following statements is most true regarding binary operations and encryption?

A. They can provide secure encryption
B. They are only useful as a teaching method
C. They can form a part of viable encryption methods
D. They are completely useless

Answer: C

NEW QUESTION 9
DES has a key space of what?

A. 2^128
B. 2^192
C. 2^64
D. 2^56

Answer: D

NEW QUESTION 10
Basic information theory is the basis for modern symmetric ciphers. Understanding the terminology of information theory is, therefore, important. If a single change of a single bit in the plaintext causes changes in all the bits of the resulting ciphertext, what is this called?

A. Complete diffusion
B. Complete scrambling
C. Complete confusion
D. Complete avalanche

Answer: D

NEW QUESTION 10
Which of the following equations is related to EC?

A. P = Cd%n
B. Me%n
C. y^2 = x^3 + Ax + B
D. Let m = (p-1)(q-1)

Answer: C

NEW QUESTION 11
Hash algortihm created by the Russians. Produces a fixed length output of 256bits. Input message is broken up into 256 bit blocks. If block is less than 256 bits then it is padded with 0s.

A. TIGER
B. GOST
C. BEAR
D. FORK-256

Answer: B

NEW QUESTION 12
Represents the total number of possible values of keys in a cryptographic algorithm or other security measure, such as a password.

A. Key Schedule
B. Key Clustering
C. Key Space
D. Key Exchange

Answer: C

NEW QUESTION 14
Which of the following is an asymmetric algorithm that was first publically described in 1977?

A. Elliptic Curve
B. Twofish
C. DESX
D. RSA

Answer: D

NEW QUESTION 16
A list of certificates that have been revoked.

A. CA
B. CRL
C. PCBC
D. OCSP

Answer: B

NEW QUESTION 20
Which one of the following are characteristics of a hash function? (Choose two)

A. Requires a key
B. One-way
C. Fixed length output
D. Symmetric
E. Fast

Answer: BC

NEW QUESTION 25
Which one of the following is a component of the PKI?

A. CA
B. TGS
C. OCSP
D. TGT

Answer: A

NEW QUESTION 29
Nicholas is working at a bank in Germany. He is looking at German standards for pseudo random number generators. He wants a good PRNG for generating symmetric keys. The German Federal Office for Information Security (BSI) has established four criteria for quality of random number generators. Which ones can be used for cryptography?

A. K4
B. K5
C. K3
D. K2
E. K1

Answer: AC

NEW QUESTION 32
You have been tasked with selecting a digital certificate standard for your company to use.
Which one of the following was an international standard for the format and information contained in a digital certificate?

A. CA
B. X.509
C. CRL
D. RFC 2298

Answer: B

NEW QUESTION 34
Cylinder tool. Wrap leather around to decode. The diameter is the key. Used in 7th century BC by greek poet Archilochus.

A. Cipher disk
B. Caesar cipher
C. Scytale
D. Enigma machine

Answer: C

NEW QUESTION 39
As a network administrator, you have implemented WPA2 encryption in your corporate wireless network. The WPA2's _____ integrity check mechanism provides security against a replay attack.

A. CBC-MAC
B. CRC-MAC
C. CRC-32
D. CBC-32

Answer: A

NEW QUESTION 43
RFC 1321 describes what hash?

A. RIPEMD
B. GOST
C. SHA1
D. MD5

Answer: D

NEW QUESTION 46
Which component of IPsec performs protocol-level functions that are required to encrypt and decrypt the packets?

A. IPsec Policy Agent
B. Internet Key Exchange (IKE)
C. Oakley
D. IPsec driver

Answer: B

NEW QUESTION 50
In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known as wardriving.
Which Algorithm is this referring to?

A. Wired Equivalent Privacy (WEP)
B. Wi-Fi Protected Access 2 (WPA2)
C. Wi-Fi Protected Access (WPA)
D. Temporal Key Integrity Protocol (TKIP)

Answer: A

NEW QUESTION 53
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

Answer: C

NEW QUESTION 57
Which of the following Secure Hashing Algorithm (SHA) produces a 160-bit digest from a message with a maximum length of (264-1) bits and resembles the MD5 algorithm?

A. SHA-0
B. SHA-2
C. SHA-1
D. SHA-3

Answer: C

NEW QUESTION 61
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

Answer: A

NEW QUESTION 63
What is a variation of DES that uses a technique called Key Whitening?

A. Blowfish
B. DESX
C. 3DES
D. AES

Answer: B

NEW QUESTION 66
John is trying to select the appropriate authentication protocol for his company. Which of the following types of authentication solutions use tickets to provide access to various resources from a central location?

A. Kerberos
B. EAP
C. Radius
D. CHAP

Answer: A

NEW QUESTION 68
Which of the following is generally true about key sizes?

A. Larger key sizes increase security
B. Key size is irrelevant to security
C. Key sizes must be more than 256 bits to be secure
D. Smaller key sizes increase security

Answer: A

NEW QUESTION 71
Which of the following acts as a verifier for the certificate authority?

A. Certificate Management system
B. Directory management system
C. Registration authority
D. Certificate authority

Answer: C

NEW QUESTION 76
Which service in a PKI will vouch for the identity of an individual or company?

A. CA
B. CR
C. KDC
D. CBC

Answer: A

NEW QUESTION 81
Which one of the following is a symmetric key system using 64-bit blocks?

A. DES
B. PGP
C. DSA
D. RSA

Answer: A

NEW QUESTION 85
A number that is used only one time, then discarded is called what?

A. IV
B. Nonce
C. Chain
D. Salt

Answer: B

NEW QUESTION 88
The time and effort required to break a security measure.

A. Session Key
B. Work factor
C. Non-repudiation
D. Payload

Answer: B

NEW QUESTION 90
Which one of the following best describes a process that splits the block of plaintext into two separate blocks, then applies the round function to one half, and finally swaps the two halves?

A. Block ciphers
B. Symmetric cryptography
C. Feistel cipher
D. Substitution cipher

Answer: C

NEW QUESTION 94
What is the basis for the difficulty in breaking RSA?

A. Hashing
B. The birthday paradox
C. Equations that describe an elliptic curve
D. Factoring numbers

Answer: D

NEW QUESTION 95
A symmetric Stream Cipher published by the German engineering firm Seimans in 1993. A software based stream cipher that uses a Lagged Fibonacci generator along with concepts borrowed from shrinking generator ciphers.

A. DESX
B. FISH
C. Twofish
D. IDEA

Answer: B

NEW QUESTION 99
All of the following are key exchange protocols except for _____

A. MQV
B. AES
C. ECDH
D. DH

Answer: B

NEW QUESTION 103
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

Answer: D

NEW QUESTION 104
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

Answer: D

NEW QUESTION 105
WPA2 uses AES for wireless data encryption at which of the following encryption levels?

A. 128 bit and CRC
B. 128 bi and TKIP
C. 128 bit and CCMP
D. 64 bit and CCMP

Answer: C

NEW QUESTION 106
_____ cryptography uses one key to encrypt a message and a different key to decrypt it.

A. Secure
B. Asymmetric
C. Stream
D. Symmetric

Answer: B

NEW QUESTION 108

.....

Relate Links

100% Pass Your 212-81 Exam with Exambible Prep Materials

https://www.exambible.com/212-81-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/