EC-Council

Exam Questions 212-81

EC-Council Certified Encryption Specialist (ECES)

NEW QUESTION 1
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

Answer: C

NEW QUESTION 2
Which of the following is a protocol for exchanging keys?

A. DH
B. EC
C. AES
D. RSA

Answer: A

NEW 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

Answer: D

NEW QUESTION 4
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 5
Denis is looking at an older system that uses DES encryption. A colleague has told him that DES is insecure due to a small key size. What is the key length used for DES?

A. 128
B. 256
C. 56
D. 64

Answer: C

NEW QUESTION 6
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 7
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 8
Which of the following is the standard for digital certificates?

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

Answer: B

NEW QUESTION 9
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 10
Which of the following algorithms uses three different keys to encrypt the plain text?

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

Answer: D

NEW QUESTION 10
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 12
The ATBASH cipher is best described as what type of cipher?

A. Asymmetric
B. Symmetric
C. Substitution
D. Transposition

Answer: C

NEW QUESTION 17
In steganography, _____ is the data to be covertly communicated (in other words, it is the message you wish to hide).

A. Carrier
B. Signal
C. Payload
D. Channel

Answer: C

NEW QUESTION 21
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 23
A _____ is a digital representation of information that identifies you as a relevant entity by a trusted third party.

A. Digital Signature
B. Hash
C. Ownership stamp
D. Digest

Answer: A

NEW QUESTION 25
Which of the following uses an 80 bit key on 64 bit blocks?

A. Skipjack
B. Twofish
C. DES
D. AES

Answer: A

NEW QUESTION 26
DES has a key space of what?

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

Answer: D

NEW QUESTION 27
Basic information theory is the basis for modern symmetric ciphers. Understanding the terminology of information theory is, therefore, important. Changes to one character in the plaintext affect multiple characters in the ciphertext. What is this referred to?

A. Avalanche
B. Confusion
C. Scrambling
D. Diffusion

Answer: D

NEW QUESTION 31
You are studying classic ciphers. You have been examining the difference between single substitution and multi-substitution. Which one of the following is an example of a multi- alphabet cipher?

A. Rot13
B. Caesar
C. Atbash
D. Vigen??re

Answer: D

NEW QUESTION 34
What is the name of the attack where the attacker obtains the ciphertexts corresponding to a set of plaintexts of his own choosing?

A. Chosen plaintext
B. Differential cryptanalysis
C. Known-plaintext attack
D. Kasiski examination

Answer: A

NEW QUESTION 35
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

Answer: A

NEW QUESTION 38
Created in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT. Most widely used public key cryptography algorithm. Based on relationships with prime numbers. This algorithm is secure because it is difficult to factor a large integer composed of two or more large prime factors.

A. PKI
B. DES

C. RSA
D. Diffie-Helmann

Answer: C

NEW QUESTION 43
With Electronic codebook (ECB) what happens:

A. The message is divided into blocks and each block is encrypted separatel
B. This is the most basic mode for symmetric encryption
C. The cipher text from the current round is XORed with the plaintext from the previous round
D. The block cipher is turned into a stream cipher
E. The cipher text from the current round is XORed with the plaintext for the next round

Answer: A

NEW QUESTION 45
Manipulating individuals so that they will divulge confidential information, rather than by breaking in or using technical cracking techniques.

A. Linear cryptanalysis
B. Replay attack
C. Side-channel attack
D. Social engineering attack

Answer: D

NEW QUESTION 48
Which of the following is a fundamental principle of cryptography that holds that the algorithm can be publicly disclosed without damaging security?

A. Vigenere's principle
B. Shamir's principle
C. Kerkchoff's principle
D. Babbage's principle

Answer: C

NEW QUESTION 49
Original, unencrypted information is referred to as _____.

A. text
B. plaintext
C. ciphertext
D. cleartext

Answer: B

NEW QUESTION 50
Protocol suite provides a method of setting up a secure channel for protected data exchange between two devices.

A. CLR
B. OCSP
C. TLS
D. IPSec

Answer: D

NEW QUESTION 51
What is the formula m^e %n related to?

A. Encrypting with EC
B. Decrypting with RSA
C. Generating Mersenne primes
D. Encrypting with RSA

Answer: D

NEW QUESTION 56
Part of understanding cryptography is understanding the cryptographic primitives that go into any crypto system. A(n) _____ is a fixed-size input to a cryptographic primitive that is random or pseudorandom.

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

Answer: A

NEW QUESTION 60
A transposition cipher invented 1918 by Fritz Nebel, used a 36 letter alphabet and a modified Polybius square with a single columnar transposition.

A. ADFVGX Cipher
B. ROT13 Cipher
C. Book Ciphers
D. Cipher Disk

Answer: A

NEW QUESTION 63
John is trying to explain the basics of cryptography to a group of young, novice, security students. Which one of the following most accurately defines encryption?

A. Changing a message using complex mathematics
B. Applying keys to a message to conceal it
C. Complex mathematics to conceal a message
D. Changing a message so it can only be easily read by the intended recipient

Answer: D

NEW QUESTION 67
In 1977 researchers and MIT described what asymmetric algorithm?

A. DH
B. RSA
C. AES
D. EC

Answer: B

NEW QUESTION 71
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 76
Asymmetric encryption method developed in 1984. It is used in PGP implementations and GNU Privacy Guard Software. Consists of 3 parts: key generator, encryption algorithm, and decryption algorithm.

A. Tiger
B. GOST
C. RIPEMD
D. ElGamal

Answer: D

NEW QUESTION 81
Which analysis type is based on the statistics of the numbers of unique colors and close- color pairs in a 24-bit image, a method that analyzes the pairs of colors created by LSB embedding?

A. Differential Analysis
B. Discrete Cosine Transform
C. Raw Quick Pair
D. Chi squared analysis

Answer: D

NEW QUESTION 82
A measure of the uncertainty associated with a random variable.

A. Collision
B. Whitening
C. Diffusion
D. Entropy

Answer: D

NEW QUESTION 83
Which one of the following uses three different keys, all of the same size?

A. 3DES
B. AES
C. RSA
D. DES

Answer: A

NEW QUESTION 88
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 93
Which of the following are valid key sizes for AES (choose three)?

A. 192
B. 56
C. 256
D. 128
E. 512
F. 64

Answer: ACD

NEW QUESTION 94
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

Answer: C

NEW QUESTION 98
What is a TGS?

A. The server that escrows keys
B. A protocol for encryption
C. A protocol for key exchange
D. The server that grants Kerberos tickets

Answer: D

NEW QUESTION 99
3DES can best be classified as which one of the following?

A. Digital signature
B. Symmetric algorithm
C. Asymmetric algorithm
D. Hashing algorithm

Answer: B

NEW QUESTION 101
Why is quantum computing a threat to RSA?

A. The processing speed will brute force algorithms
B. Quantum computers can solve the discrete logarithm problem
C. Quantum computers can solve the birthday paradox
D. Quantum computers can factor large integers in polynomial time

Answer: D

NEW QUESTION 102
The art and science of writing hidden messages so that no one suspects the existence of the message, a type of security through obscurity. Message can be

hidden in picture or audio file for example. Uses least significant bits in a file to store data.

A. Steganography
B. Cryptosystem
C. Avalanche effect
D. Key Schedule

Answer: A

NEW QUESTION 106
A _____ is a function that takes a variable-size input m and returns a fixed-size string.

A. Feistel
B. Asymmetric cipher
C. Symmetric cipher
D. Hash

Answer: D

NEW QUESTION 109
A non-secret binary vector used as the initializing input algorithm for encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance.

A. IV
B. Salt
C. L2TP
D. Nonce

Answer: A

NEW QUESTION 112
A technique used to increase the security of block ciphers. It consists of steps that combine the data with portions of the key (most commonly using a simple XOR) before the first round and after the last round of encryption.

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

Answer: A

NEW QUESTION 114
You are trying to find a modern method for security web traffic for use in your company's ecommerce web site. Which one of the following is used to encrypt web pages and uses bilateral authentication?

A. AES
B. SSL
C. TLS
D. 3DES

Answer: C

NEW QUESTION 115
RFC 1321 describes what hash?

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

Answer: D

NEW QUESTION 118
A cryptographic hash function which uses a Merkle tree-like structure to allow for immense parallel computation of hashes for very long inputs. Authors claim a performance of 28 cycles per byte for MD6-256 on an Intel Core 2 Duo and provable resistance against differential cryptanalysis.

A. TIGER
B. GOST
C. MD5
D. MD6

Answer: D

NEW QUESTION 121
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

Answer: A

NEW QUESTION 126
Used to take the burden off of a CA by handling verification prior to certificates being issued. Acts as a proxy between user and CA. Receives request, authenticates it and forwards it to the CA.

A. PKI (Public Key Infrastructure)
B. TTP (Trusted Third Party)
C. RA (Registration Authority)
D. CP (Certificate Policy)

Answer: C

NEW QUESTION 130
Which of the following is not a key size used by AES?

A. 128 bits
B. 192 bits
C. 256 bits
D. 512 b

Answer: D

NEW QUESTION 131
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 133
The next number is derived from adding together the prior two numbers (1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89).

A. Odd numbers
B. Fibonacci Sequence
C. Fermat pseudoprime
D. Prime numbers

Answer: B

NEW QUESTION 134
Message hidden in unrelated text. Sender and receiver have pre-arranged to use a pattern to remove certain letters from the message which leaves only the true message behind.

A. Caesar Cipher
B. Null Ciphers
C. Vigenere Cipher
D. Playfair Cipher

Answer: B

NEW QUESTION 139
What size block does AES work on?

A. 64
B. 128
C. 192
D. 256

Answer: B

NEW QUESTION 142
Which one of the following is an algorithm that uses variable length key from 1 to 256 bytes, which constitutes a state table that is used for subsequent generation of pseudorandom bytes and then a pseudorandom string of bits, which is XORed with the plaintext to produce the ciphertext?

A. PIKE
B. Twofish
C. RC4
D. Blowfish

Answer: C

NEW QUESTION 143
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 145
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 150
Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?

A. Key distribution
B. Security
C. Scalability
D. Speed

Answer: D

NEW QUESTION 154
Which one of the following attempts to hide data in plain view?

A. Cryptography
B. Substitution
C. Steganography
D. Asymmetric cryptography

Answer: C

NEW QUESTION 159
Software for maintaining an on-the-fly-encrypted volume. Data is automatically encrypted right before it is saved, then decrypted right after it is loaded, all w/o user intervention.

A. VPN
B. PGP
C. Cryptool
D. VeraCrypt

Answer: D

NEW QUESTION 161
Uses a formula, M_n = 2^n 1 where n is a prime number, to generate primes. Works for 2, 3, 5, 7 but fails on 11 and on many other n values.

A. Fibonacci Numbers
B. Co-prime Numbers
C. Even Numbers
D. Mersenne Primes

Answer: D

NEW QUESTION 164
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

Answer: C

NEW QUESTION 167
In IPSec, if the VPN is a gateway-gateway or a host-gateway, then which one of the following is true?

A. IPSec does not involve gateways
B. Only transport mode can be used
C. Encapsulating Security Payload (ESP) authentication must be used
D. Only the tunnel mode can be used

Answer: D

NEW QUESTION 172
The most widely used asymmetric encryption algorithm is what?

A. Vigenere
B. Caesar Cipher
C. RSA
D. DES

Answer: C

NEW QUESTION 177
Which of the following is used to encrypt email and create digital signatures?

A. DES
B. SHA1
C. AES
D. RSA

Answer: D

NEW QUESTION 179
A _____ product refers to an NSA-endorsed classified or controlled cryptographic item for classified or sensitive U. S. government information, including cryptographic equipment, assembly, or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed

A. 1
B. 4
C. 2
D. 3

Answer: A

NEW QUESTION 183
In a _____ the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key.

A. Information deduction
B. Total break
C. Instance deduction
D. Global deduction

Answer: B

NEW QUESTION 187
In relationship to hashing, the term _____ refers to random bits that are used as one of the inputs to the hash. Essentially the _____ is intermixed with the message that is to be hashed

A. Vector
B. Salt
C. Stream
D. IV

Answer: B

NEW QUESTION 190
John works as a cryptography consultant. He finds that people often misunderstand the reality of breaking a cipher. What is the definition of breaking a cipher?

A. Finding any method that is more efficient than brute force
B. Uncovering the algorithm used
C. Rendering the cypher no longer useable
D. Decoding the key

Answer: A

NEW QUESTION 192
Changing some part of the plain text for some matching part of cipher text. Historical algorithms typically use this.

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

Answer: B

NEW QUESTION 197
Which of the following is the successor of SSL?

A. GRE
B. RSA
C. IPSec
D. TLS

Answer: D

NEW QUESTION 199
A cipher is defined as what

A. The algorithm(s) needed to encrypt and decrypt a message
B. Encrypted text
C. The key used to encrypt a message
D. Any algorithm used in cryptography

Answer: A

NEW QUESTION 204
Which one of the following wireless standards uses the Advanced Encryption Standard (AES) using the Counter Mode-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP)?

A. WEP
B. WEP2
C. WPA
D. WPA2

Answer: D

NEW QUESTION 205
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 208
A protocol for key aggreement based on Diffie-Hellman. Created in 1995. Incorporated into the public key standard IEEE P1363.

A. Blum Blum Shub
B. Elliptic Curve
C. Menezes-Qu-Vanstone
D. Euler's totient

Answer: C

NEW QUESTION 211
Which algorithm implements an unbalanced Feistel cipher?

A. Skipjack
B. RSA
C. 3DES
D. Blowfish

Answer: A

NEW QUESTION 213

Calculates the average LSB and builds a table of frequencies and Pair of Values. Performs a test on the two tables. It measures the theoretical vs. calculated population difference.

A. Certificate Authority
B. Raw Quick Pair
C. Chi-Square Analysis
D. SP network

Answer: C

NEW QUESTION 216
Bruce Schneier is a well-known and highly respected cryptographer. He has developed several pseudo random number generators as well as worked on teams developing symmetric ciphers. Which one of the following is a symmetric block cipher designed in 1993 by Bruce Schneier team that is unpatented?

A. Pegasus
B. Blowfish
C. SHA1
D. AES

Answer: B

NEW QUESTION 217
MD5 can best be described as which one of the following?

A. Asymmetric algorithm
B. Hashing algorithm
C. Digital signature
D. Symmetric algorithm

Answer: B

NEW QUESTION 221
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 225
What is a salt?

A. Key whitening
B. Random bits intermixed with a symmetric cipher to increase randomness and make it more secure
C. Key rotation
D. Random bits intermixed with a hash to increase randomness and reduce collisions

Answer: D

NEW QUESTION 226
What size block does Skipjack use?

A. 64
B. 512
C. 128
D. 256

Answer: A

NEW QUESTION 228
Jane is looking for an algorithm to ensure message integrity. Which of following would be an acceptable choice?

A. RSA
B. AES
C. RC4
D. SHA-1

Answer: D

NEW QUESTION 231
A linear congruential generator is an example of what?

A. A coprime generator
B. A prime number generator
C. A pseudo random number generator
D. A random number generator

Answer: C

NEW QUESTION 236
If you XOR 10111000 with 10101010, what is the result?

A. 10111010
B. 10101010
C. 11101101
D. 00010010

Answer: D

NEW QUESTION 240
Which of the following encryption algorithms relies on the inability to factor large prime numbers?

A. RSA
B. MQV
C. EC
D. AES

Answer: A

NEW QUESTION 245
A cryptanalysis success where the attacker discovers additional plain texts (or cipher texts) not previously known.

A. Total Break
B. Distinguishing Algorithm
C. Instance Deduction
D. Information Deduction

Answer: C

NEW QUESTION 248
A simple algorithm that will take the initial key and from that generate a slightly different key each round.

A. Key Schedule
B. Feistel Network
C. SHA-2
D. Diffie-Helman

Answer: A

NEW QUESTION 253
This algorithm was published by the German engineering firm Seimans in 1993. It is a software based stream cipher using Lagged Fibonacci generator along with a concept borrowed from the shrinking generator ciphers.

A. RC4
B. Blowfish
C. Twofish
D. FISH

Answer: D

NEW QUESTION 258
Which one of the following wireless standards uses AES using the Counter Mode-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP)?

A. WEP2
B. WPA
C. WEP
D. WPA2

Answer: D

NEW QUESTION 263
If you use substitution alone, what weakness is present in the resulting cipher text?

A. It is the same length as the original text
B. It is easily broken with modern computers
C. It maintains letter and word frequency

D. It is too simple

Answer: C

NEW QUESTION 267
A type of frequency analysis used to attack polyalphabetic substitution ciphers. It's used to try to discover patterns and use that information to decrypt the cipher.

A. Kasiski Method
B. Birthday Attack
C. Information Deduction
D. Integral Cryptanalysis

Answer: A

NEW QUESTION 272
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 273
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 275
Ahlen is using a set of pre-calculated hashes to attempt to derive the passwords from a Windows SAM file. What is a set of pre-calculated hashes used to derive a hashed password called?

A. Hash matrix
B. Rainbow table
C. Password table
D. Hash table

Answer: B

NEW QUESTION 277
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

Answer: D

NEW QUESTION 282
Which one of the following is an example of a symmetric key algorithm?

A. ECC
B. Diffie-Hellman
C. RSA
D. Rijndael

Answer: D

NEW QUESTION 285
Which of the following is an asymmetric algorithm related to the equation y^2 = x^3 + Ax + B?

A. Blowfish
B. Elliptic Curve
C. AES
D. RSA

Answer: B

NEW QUESTION 286
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

Answer: C

NEW QUESTION 289
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

212-81 Practice Exam Features:

* 212-81 Questions and Answers Updated Frequently

* 212-81 Practice Questions Verified by Expert Senior Certified Staff

* 212-81 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 212-81 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year