EC-Council

Exam Questions 212-81

EC-Council Certified Encryption Specialist (ECES)

NEW QUESTION 1
Which of the following is a type of encryption that has two different keys. One key can encrypt the message and the other key can only decrypt it?

A. Block cipher
B. Asymmetric
C. Symmetric
D. Stream cipher

Answer: B

NEW QUESTION 2
In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?

A. Keyed Hashing
B. Double Hashing
C. Salting
D. Key Stretching

Answer: C

NEW QUESTION 3
What must occur in order for a cipher to be considered ??broken???

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

Answer: C

NEW QUESTION 4
What type of encryption uses different keys to encrypt and decrypt the message?

A. Asymmetric
B. Symmetric
C. Secure
D. Private key

Answer: A

NEW QUESTION 5
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 6
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 7
Bob??s password is hashed, and so is John??s. Even though they used different passwords, the hash is the same. What is this called?

A. A collision
B. A mistake
C. Convergence
D. Transposition

Answer: A

NEW QUESTION 8
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 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
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 10
The ATBASH cipher is best described as what type of cipher?

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

Answer: C

NEW QUESTION 12
Which one of the following terms describes two numbers that have no common factors?

A. Coprime
B. Fermat's number
C. Euler's totient
D. Convergent

Answer: A

NEW QUESTION 15
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 18
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 21
Collision resistance is an important property for any hashing algorithm. Joan wants to find a cryptographic hash that has strong collision resistance. Which one of the following is the most collisionresistant?

A. SHA2

B. MD5
C. MD4
D. PIKE

Answer: A

NEW QUESTION 23
What does the OCSP protocol provide?

A. Revoked certificates
B. Hashing
C. VPN connectivity
D. Encryption

Answer: A

NEW QUESTION 28
What is the largest key size that AES can use?

A. 256
B. 56
C. 512
D. 128

Answer: A

NEW QUESTION 30
How many qubits are needed to break RSA?

A. 1000
B. 2000
C. 4000
D. 100

Answer: C

NEW QUESTION 34
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 35
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 39
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 44
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 49
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 54
If the round function is a cryptographically secure pseudorandom function, then _____ rounds is sufficient to make the block cipher a pseudorandom permutation.

A. 2
B. 15
C. 16
D. 3

Answer: D

NEW QUESTION 55
Original, unencrypted information is referred to as _____.

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

Answer: B

NEW QUESTION 59
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 61
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 66
What is Kerchoff's principle?

A. A minimum of 15 rounds is needed for a Feistel cipher to be secure
B. Only the key needs to be secret, not the actual algorithm
C. Both algorithm and key should be kept secret
D. A minimum key size of 256 bits is necessary for security

Answer: B

NEW QUESTION 68
Juanita is attempting to hide some text into a jpeg file. Hiding messages inside another medium is referred to as which one of the following?

A. Cryptography
B. Steganalysis
C. Cryptology
D. Steganography

Answer: D

NEW QUESTION 69
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 72
When learning algorithms, such as RSA, it is important to understand the mathematics being used. In RSA, the number of positive integers less than or equal to some number is critical in key generation. The number of positive integers less than or equal to n that are coprime to n is called _____.

A. Mersenne's number
B. Fermat's number
C. Euler's totient
D. Fermat's prime

Answer: C

NEW QUESTION 75
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 78
In 1977 researchers and MIT described what asymmetric algorithm?

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

Answer: B

NEW QUESTION 80
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
What is the basis for the FISH algorithm?

A. The Lagged Fibonacci generator
B. Prime number theory
C. Equations that describe an ellipse
D. The difficulty in factoring numbers

Answer: A

NEW QUESTION 83
If the round function is a cryptographically secure pseudorandom function, then _____ rounds is sufficient to make it a "strong" pseudorandom permutation.

A. 15
B. 16
C. 3
D. 4

Answer: D

NEW QUESTION 86
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 90
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 95
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 96
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 99
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 102
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 106
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 110
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
Which of the following is a block cipher?

A. AES
B. DH
C. RC4
D. RSA

Answer: A

NEW QUESTION 120
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 121
Frank is trying to break into an encrypted file?? He is attempting all the possible keys that could be used for this algorithm. Attempting to crack encryption by simply trying as many randomly generated keys as possible is referred to as what?

A. Rainbow table
B. Frequency analysis
C. Brute force
D. Kasiski

Answer: C

NEW QUESTION 125
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 128
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 133
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 135
If Bob is using asymmetric cryptography and wants to send a message to Alice so that only she can decrypt it, what key should he use to encrypt the message?

A. Alice's private key
B. Bob's private key
C. Alice's public key
D. Bob's public key

Answer: C

NEW QUESTION 139
A symmetric block cipher designed in 1993 by Bruce Schneier. Was intended as a replacement for DES. Like DES it is a 16 round Feistel working on 64bit blocks. Can have bit sizes 32bits to 448bits.

A. Skipjack
B. Blowfish
C. MD5
D. Serpent

Answer: B

NEW QUESTION 141
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 146
What size block does AES work on?

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

Answer: B

NEW QUESTION 149
_____ uses at least two different shifts, changing the shift with different letters in the plain text.

A. Caesar cipher
B. multi-alphabet encryption
C. Scytale
D. Atbash

Answer: B

NEW QUESTION 153
Algorithm that was chosen for the Data Encryption Standard, which was altered and renamed Data Encryption Algorithm.

A. Blowfish
B. Rijndael
C. Lucifer
D. El Gamal

Answer: C

NEW QUESTION 157
The mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext.

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

Answer: C

NEW QUESTION 158
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 161
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 162
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 164
Which of the following would be the fastest.

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

Answer: D

NEW QUESTION 169
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 172
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 176
Symmetric algorithm. Designed by James Massey and Xuejia Lai. Operates on 64 bit blocks and has a 128 bit key. Consists of 8 identical transformations each round and an output transformation.

A. IDEA
B. RSA
C. CAST
D. DES

Answer: A

NEW QUESTION 177
Numbers that have no factors in common with another.

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

Answer: C

NEW QUESTION 180
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 184
Ferris has been assigned the task of selecting security for his company's wireless network. It is important that he pick the strongest form of wireless security. Which one of the following is the strongest wireless security?

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

Answer: C

NEW QUESTION 185
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 188
Fred is using an operating system that stores all passwords as an MD5 hash. What size is an MD5 message digest (hash)?

A. 160
B. 512
C. 256
D. 128

Answer: D

NEW QUESTION 192
During the process of encryption and decryption, what keys are shared?

A. Public keys
B. Public and private keys
C. User passwords
D. Private keys

Answer: A

NEW QUESTION 197
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 198
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 199
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 203
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 206
Network of trusted certificate authority servers. Use asymmetric key pairs and combines software, encryption and services to provide a means of protecting security of business communication and transactions.

A. PKI
B. GOST
C. CA
D. PIKE

Answer: A

NEW QUESTION 210
Ciphers that write message letters out diagonally over a number of rows then read off cipher row by row. Also called zig-zag cipher.

A. Rail Fence Cipher
B. Null Cipher
C. Vigenere Cipher
D. ROT-13

Answer: A

NEW QUESTION 213
Which of the following is the successor of SSL?

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

Answer: D

NEW QUESTION 215
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 216
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 220
Which algorithm implements an unbalanced Feistel cipher?

A. Skipjack

B. RSA
C. 3DES
D. Blowfish

Answer: A

NEW QUESTION 224
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 226
Cryptographic hashes are often used for message integrity and password storage. It is important to understand the common properties of all cryptographic hashes. What is not true about a hash?

A. Few collisions
B. Reversible
C. Variable length input
D. Fixed length output

Answer: B

NEW QUESTION 227
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 228
If you XOR 10111000 with 10101010, what is the result?

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

Answer: D

NEW QUESTION 229
An authentication method that periodically re-authenticates the client by establishing a hash that is then resent from the client is called _____ .

A. CHAP
B. SPAP
C. PAP
D. EAP

Answer: A

NEW QUESTION 232
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 233
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 234
Hash. Created by Ronald Rivest. Replaced MD4. 128 bit output size, 512 bit block size, 32 bit word size, 64 rounds. Infamously compromised by Flame malware in 2012.

A. Keccak
B. MD5
C. SHA-1
D. TIGER

Answer: B

NEW QUESTION 235
Which of the following is assured by the use of a hash?

A. Confidentiality
B. Availability
C. Authentication
D. Integrity

Answer: D

NEW QUESTION 240
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 241
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 243
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 245
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 249
.....

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