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
What is the solution to the equation 8 mod 3?

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

Answer: D

NEW QUESTION 3
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 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
Which of the following is a protocol for exchanging keys?

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

Answer: A

NEW QUESTION 6
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 7
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 8
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 9
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 10
What does Output feedback (OFB) do:

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. A block cipher is converted into a stream cipher by generating a keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext
E. The cipher text from the current round is XORed with the plaintext for the next round

Answer: C

NEW QUESTION 10
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 12
Which of the following is the standard for digital certificates?

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

Answer: B

NEW QUESTION 17
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 20
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 24
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 25
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 26
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 30
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 32
What is the largest key size that AES can use?

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

Answer: A

NEW QUESTION 36
DES has a key space of what?

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

Answer: D

NEW QUESTION 38
Encryption of the same plain text with the same key results in the same cipher text. Use of an IV that is XORed with the first block of plain text solves this problem.

A. CFB
B. GOST
C. ECB
D. RC4

Answer: C

NEW QUESTION 39
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 41
You are explaining basic mathematics to beginning cryptography students. You are covering the basic math used in RSA. A prime number is defined as

A. Odd numbers with no divisors
B. Odd numbers
C. Any number only divisible by odd numbers
D. Any number only divisible by one and itself

Answer: C

NEW QUESTION 43
A digital document that contains a public key and some information to allow your system to verify where that key came from. Used for web servers, Cisco Secure phones, E- Commerce.

A. Registration Authority
B. Payload
C. OCSP
D. Digital Certificate

Answer: D

NEW QUESTION 46
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 48
With Cipher-block chaining (CBC) what happens?

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

Answer: C

NEW QUESTION 53
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 54
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 55
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 60
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 64
How does Kerberos generate the first secret key in the authentication process?

A. By generating a random AES key
B. By creating a hash of the user password
C. By hashing the user ID, network I
D. and salt
E. By using the user's public key

Answer: B

NEW QUESTION 68
In order to understand RSA. you must understand the key generation algorithm as well as the encryption and decryption algorithms. Which one of the following equations describes the encryption process for RSA?

A. Me mod n
B. Ce mod n
C. y2 = x3 + Ax + B
D. P = Cd mod n

Answer: B

NEW QUESTION 73
Modern symmetric ciphers all make use of one or more s-boxes. Both Feistel and non- Feistel ciphers use these s-boxes. What is an s-box?

A. A substitution box where input bits are replaced
B. A black box for the algorithm implementation
C. A shifting box where input bits are shifted
D. Another name for the round function

Answer: A

NEW QUESTION 77
Original, unencrypted information is referred to as _____.

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

Answer: B

NEW QUESTION 79
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 83
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 85
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 89
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 91
In 1977 researchers and MIT described what asymmetric algorithm?

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

Answer: B

NEW QUESTION 96
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 98
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 102
Which one of the following is a component of the PKI?

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

Answer: A

NEW QUESTION 107
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 110
Which of the following techniques is used (other than brute force) to attempt to derive a key?

A. Cryptography
B. Cryptoanalysis
C. Password cracking
D. Hacking

Answer: B

NEW QUESTION 111
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 115
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 119
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 120
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 123
John is going to use RSA to encrypt a message to Joan. What key should he use?

A. A random key
B. Joan??s public key
C. A shared key
D. Joan??s private key

Answer: B

NEW QUESTION 125
RFC 1321 describes what hash?

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

Answer: D

NEW QUESTION 127
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 128
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 133
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 138
Which one of the following is an authentication method that sends the username and password in cleartext?

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

Answer: A

NEW QUESTION 143
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 144
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 149
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 153
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 157
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 161
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 164
What size block does AES work on?

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

Answer: B

NEW QUESTION 165
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 167
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 169
Which of the following would be the fastest.

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

Answer: D

NEW QUESTION 173
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 177
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 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 183
The most widely used asymmetric encryption algorithm is what?

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

Answer: C

NEW QUESTION 184
What advantage do symmetric algorithms have over asymmetric algorithms

A. It is easier to implement them in software
B. They are more secure
C. They are fasterD It is easier to exchange keys

Answer: C

NEW QUESTION 187
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 189
The most widely used digital certificate standard. First issued July 3, 1988. It is a digital document that contains a public key signed by the trusted third party, which is known as a Certificate Authority, or CA. Relied on by S/MIME. Contains your name, info about you, and a signature of a person who issued the certificate.

A. ElGamal
B. RSA
C. PAP
D. X.509

Answer: D

NEW QUESTION 194
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 195
How did the ATBASH cipher work?

A. By substituting each letter for the letter from the opposite end of the alphabet (i.
B. A becomes Z, B becomes Y, etc.)
C. By rotating text a given number of spaces
D. By Multi alphabet substitution
E. By shifting each letter a certain number of spaces

Answer: A

NEW QUESTION 200
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 205
How can rainbow tables be defeated?

A. Lockout accounts under brute force password cracking attempts
B. All uppercase character passwords
C. Use of non-dictionary words
D. Password salting

Answer: D

NEW QUESTION 208
If you XOR 10111000 with 10101010, what is the result?

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

Answer: D

NEW QUESTION 209
Which of the following would be the weakest encryption algorithm?

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

Answer: A

NEW QUESTION 214
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 218
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 220
Which of the following is assured by the use of a hash?

A. Confidentiality
B. Availability
C. Authentication

D. Integrity

Answer: D

NEW QUESTION 223
In a Feistel cipher, the two halves of the block are swapped in each round. What does this provide?

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

Answer: C

NEW QUESTION 224
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

Answer: BC

NEW QUESTION 227
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 231
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 236
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 238
.....

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