# 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**
What is the solution to the equation 8 mod 3?

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

**Answer:** D

**NEW QUESTION 2**
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 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**
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 5**
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 6**
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 7**
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 8**
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 9**
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 10**
What is the largest key size that AES can use?

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

**Answer:** A

**NEW QUESTION 10**
The concept that if one bit of data changes, the cipher text will all completely change as well.

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

**Answer:** A

**NEW QUESTION 15**
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 19**
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 23**
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 26**
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 29**
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 30**
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 32**
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 36**
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 38**
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 42**
Which of the following is required for a hash?

A. Not vulnerable to a brute force attack
B. Few collisions
C. Must use SALT
D. Not reversible
E. Variable length input, fixed length output
F. Minimum key length

**Answer:** DE

**NEW QUESTION 44**
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 45**
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 50**
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 55**
A list of certificates that have been revoked.

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

**Answer:** B

**NEW QUESTION 58**
In 1977 researchers and MIT described what asymmetric algorithm?

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

**Answer:** B

**NEW QUESTION 61**
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 62**
Which one of the following is a component of the PKI?

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

**Answer:** A

**NEW QUESTION 66**
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 71**
A measure of the uncertainty associated with a random variable.

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

**Answer:** D

**NEW QUESTION 76**
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 78**
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 79**
Early attempt to make substitution ciphers more robust, masks letter frequencies, plain text letters map to multiple cipher text symbols.

A. Scytale Cipher
B. Playfair Cipher
C. Homophonic Substitution
D. ADFVGX Cipher

**Answer:** C

**NEW QUESTION 81**
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 84**
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 88**
Which of the following is an asymmetric cipher?

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

**Answer:** A

**NEW QUESTION 89**
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 90**
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 91**
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 93**
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 97**
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 100**
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 102**
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 107**
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 112**
Terrance oversees the key escrow server for his company. All employees use asymmetric cryptography to encrypt all emails. How many keys are needed for asymmetric cryptography?

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

**Answer:** A

**NEW QUESTION 114**
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 117**
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 119**
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 124**
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 126**
Developed by Netscape and has been replaced by TLS. It was the preferred method used with secure websites.

A. OCSP
B. VPN
C. CRL
D. SSL

**Answer:** D

**NEW QUESTION 128**
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 133**
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 137**
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 139**
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 142**
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 145**
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 148**
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 149**
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 153**
Created by D. H. Lehmer. It is a classic example of a Linear congruential generator. A PRNG type of linear congruential generator (LCG) that operates in multiplicative group of integers modulo n. The basic algorithm is Xi+1=(aXi + c) mod m, with 0 Xi m.

A. Lehmer Random Number Generator
B. Lagged Fibonacci Generator
C. Linear Congruential Generator
D. Blum Blum Shub

**Answer:** A

**NEW QUESTION 155**
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 160**
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 161**
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 164**
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 166**
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 169**
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 172**
A cryptanalysis success where the attacker deduces the secret key.

A. Information Deduction
B. Avalanche effect
C. Shannon's Entropy
D. Total Break

**Answer:** D

**NEW QUESTION 176**
Which algorithm implements an unbalanced Feistel cipher?

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

**Answer:** A

**NEW QUESTION 180**
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 185**
A _____ is a function is not reversible.

A. Stream cipher
B. Asymmetric cipher
C. Hash
D. Block Cipher

**Answer:** C

**NEW QUESTION 188**
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 191**
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 196**
If you XOR 10111000 with 10101010, what is the result?

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

**Answer:** D

**NEW QUESTION 201**
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 206**
What size key does Skipjack use?

A. 128 bit
B. 56 bit
C. 80 bit
D. 256 bit

**Answer:** C

**NEW QUESTION 211**
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 212**
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 216**
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 219**
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 224**
Electromechanical rotor-based cipher used in World War II

A. ROT13 Cipher
B. Cipher Disk
C. Enigma Machine
D. Rail Fence Cipher

**Answer:** C

**NEW QUESTION 227**
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 228**
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 231**
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 232**
.....

# 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/