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
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 3
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 4
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 5
What is the largest key size that AES can use?

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

Answer: A

NEW QUESTION 6
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 7
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 8
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 9
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 10
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 10
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 14
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 17
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 19
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 24
A list of certificates that have been revoked.

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

Answer: B

NEW QUESTION 29
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 30
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 34
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 38
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 39
Which of the following is an asymmetric cipher?

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

Answer: A

NEW QUESTION 42
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 43
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 48
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 52
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 55
What size block does FORK256 use?

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

Answer: B

NEW QUESTION 58
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 61
Which of the following would be the fastest.

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

Answer: D

NEW QUESTION 66
Which of the following asymmetric algorithms is described by U.S. Patent 5,231,668 and FIPS 186

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

Answer: C

NEW QUESTION 69
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 73
The most widely used asymmetric encryption algorithm is what?

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

Answer: C

NEW QUESTION 76
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 79
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 83
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 87
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 89
Which algorithm implements an unbalanced Feistel cipher?

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

Answer: A

NEW QUESTION 93
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 96

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

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

Answer: D

NEW QUESTION 101
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 106
Storing private keys with a third party is referred to as what?

A. Key caching
B. Key storage
C. Key banking
D. Key escrow

Answer: D

NEW QUESTION 110
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 114
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 115
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 116
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 120
.....

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