Exam Questions 212-81

EC-Council Certified Encryption Specialist (ECES)

https://www.2passeasy.com/dumps/212-81/

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
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 3
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 4
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 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
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 7
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 8
The ATBASH cipher is best described as what type of cipher?

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

Answer: C

NEW QUESTION 9
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 10
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 10
The most common way steganography is accomplished is via which one of the following?

A. rsb
B. lsb
C. msb
D. asb

Answer: B

NEW QUESTION 11
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 12
What does the OCSP protocol provide?

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

Answer: A

NEW QUESTION 16
What is the largest key size that AES can use?

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

Answer: A

NEW QUESTION 20
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 22
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 26
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 31
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 32
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 35
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 36
Which method of password cracking takes the most time and effort?

A. Dictionary attack
B. Shoulder surfing
C. Brute force
D. Rainbow tables

Answer: C

NEW QUESTION 37
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 41
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 46
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 49
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 53
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 54
A measure of the uncertainty associated with a random variable.

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

Answer: D

NEW QUESTION 58
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 63
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 67
RFC 1321 describes what hash?

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

Answer: D

NEW QUESTION 71
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 74
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 75
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 79
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 81
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 84
This is a proprietary version of PAP. Encrypts username and password as it is sent across network.

A. PPTP VPN

B. S-PAP
C. Kerberos
D. WPA2

Answer: B

NEW QUESTION 87
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 90
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 93
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 98
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 101
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 105
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 109
With Cipher feedback (CFB) what happens?

A. The key is reapplied
B. The ciphertext block is encrypted then the ciphertext produced is XOR??d back with the plaintext to produce the current ciphertext block
C. The block cipher is turned into a stream cipher

D. The message is divided into blocks and each block is encrypted separatel
E. This is the most basic mode for symmetric encryption

Answer: B

NEW QUESTION 110
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 112
The most widely used asymmetric encryption algorithm is what?

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

Answer: C

NEW QUESTION 116
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 117
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 119
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 120
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 123
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 126
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 128
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 131
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 136
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 140
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 143
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 144
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 146
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 147
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 148
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 212-81 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 212-81 Product From:

https://www.2passeasy.com/dumps/212-81/

Money Back Guarantee

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