212-81 Q&As

EC-Council Certified Encryption Specialist (ECES)

Pass EC-COUNCIL 212-81 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/212-81.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

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

Correct Answer: A

SHA2 https://en.wikipedia.org/wiki/Collision_resistance Collision resistance is a property of cryptographic hash functions: a hash function H is collision-resistant if it is hard to find two inputs that hash to the same output; that is, two inputs a and b where a b but H(a) = H(b). The pigeonhole principle means that any hash function with more inputs than outputs will necessarily have such collisions; the harder they are to find, the more cryptographically secure the hash function is. Due to the Birthday Problem, for a hash function that produces an output of length n bits, the probability of getting a collision is 1/2^n/2. So, just looking for a hash function with larger "n". The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA- 512/256.

QUESTION 2

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

Correct Answer: B

MD5 https://en.wikipedia.org/wiki/MD5 The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database. MD5 was designed by Ronald Rivest in 1991 to replace an earlier hash function MD4, and was specified in 1992 as RFC 1321

QUESTION 3

Which algorithm implements an unbalanced Feistel cipher?

A. Skipjack

B. RSA

C. 3DES

D. Blowfish

Correct Answer: A

Skipjack

https://en.wikipedia.org/wiki/Skipjack_(cipher)

Skipjack uses an 80-bit key to encrypt or decrypt 64-bit data blocks. It is an unbalanced Feistel network with 32 rounds.

QUESTION 4

Which of the following would be the weakest encryption algorithm?

A. DES

B. AES

C. RSA

D. EC

Correct Answer: A

DES https://en.wikipedia.org/wiki/Data_Encryption_Standard DES is insecure due to the relatively short 56-bit key size. In January 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes.

QUESTION 5

Which of the following is an asymmetric cipher?

A. RSA

B. AES

C. DES

D. RC4

Correct Answer: A

RSA

https://en.wikipedia.org/wiki/RSA_(cryptosystem)

RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who

publicly described the algorithm in 1977. An equivalent system was developed secretly, in 1973 at GCHQ (the British signals intelligence agency), by the English mathematician Clifford Cocks. That system was declassified in 1997.

In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value.

The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

QUESTION 6

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

Correct Answer: C

DSA https://ru.wikipedia.org/wiki/DSA The National Institute of Standards and Technology (NIST) proposed DSA for use in their Digital Signature Standard (DSS) in 1991, and adopted it as FIPS 186 in 1994. DSA is covered by U.S. Patent 5,231,668 , filed July 26, 1991 and now expired, and attributed to David W. Kravitz, a former NSA employee.

QUESTION 7

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

Correct Answer: A

Finding any method that is more efficient than brute force.

https://en.wikipedia.org/wiki/Cryptanalysis

Bruce Schneier notes that even computationally impractical attacks can be considered breaks: "Breaking a cipher simply means finding a weakness in the cipher that can be exploited with a complexity less than brute force. Never mind that

brute-force might require 2^128 encryptions; an attack requiring 2^110 encryptions would be considered a break...simply put, a break can just be a certificational weakness: evidence that the cipher does not perform as

advertised."

QUESTION 8

Numbers that have no factors in common with another.

A. Fibonacci Numbers

B. Even Numbers

C. Co-prime numbers

D. Mersenne Primes

Correct Answer: C

Correct answers: Co-prime numbers https://en.wikipedia.org/wiki/Coprime_integers Two integers a and b are said to be relatively prime, mutually prime, or coprime if the only positive integer (factor) that evenly divides both of them is 1. Consequently, any prime number that divides one of a or b does not divide the other. This is equivalent to their greatest common divisor (gcd) being 1. The numerator and denominator of a reduced fraction are coprime. The numbers 14 and 25 are coprime, since 1 is their only common divisor. On the other hand, 14 and 21 are not coprime, because they are both divisible by 7.

QUESTION 9

Which of the following is an asymmetric algorithm that was first publically described in 1977?

A. Elliptic Curve

B. Twofish

C. DESX

D. RSA

Correct Answer: D

RSA

https://en.wikipedia.org/wiki/RSA_(cryptosystem)

RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who

publicly described the algorithm in 1977.

QUESTION 10

Which of the following are valid key sizes for AES (Choose three)?

A. 192

B. 56

C. 256

D. 128

E. 512

F. 64

Correct Answer: ACD

Correct answers: 128, 192, 256 https://en.wikipedia.org/wiki/Advanced_Encryption_Standard The Advanced Encryption Standard (AES), also known by its original name Rijndael, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

QUESTION 11

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

Correct Answer: A

Type 1 https://en.wikipedia.org/wiki/NSA_cryptography#Type_1_Product A Type 1 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.

QUESTION 12

Which one of the following is a component of the PKI?

A. CA

B. TGS

C. OCSP

D. TGT

Correct Answer: A

CA https://en.wikipedia.org/wiki/Certificate_authority Certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party--trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 or EMV standard.

QUESTION 13

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

Correct Answer: B

Salt

https://en.wikipedia.org/wiki/Salt_(cryptography)

A salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but

over time additional safeguards were developed to protect a user\\'s password against being read from the system. A salt is one of those methods.

QUESTION 14

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

Correct Answer: A

DSA https://en.wikipedia.org/wiki/Digital_Signature_Algorithm DSA is covered by U.S. Patent 5,231,668 , filed July 26, 1991 and now expired, and attributed to David W. Kravitz, a former NSA employee. This patent was given to "The United States of America as represented by the Secretary of Commerce, Washington, D.C.", and NIST has made this

patent available worldwide royalty-free. Claus P. Schnorr claims that his U.S. Patent 4,995,082 (also now expired) covered DSA; this claim is disputed.

QUESTION 15

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 separately. This is the most basic mode for symmetric encryption

Correct Answer: B

The ciphertext block is encrypted then the ciphertext produced is XOR\\'d back with the plaintext to produce the current ciphertext block https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Cipher_feedback_(CFB) The cipher feedback (CFB) mode, a close relative of CBC, makes a block cipher into a self- synchronizing stream cipher.