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.pass2lead.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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

Correct Answer: D

Correct answers: Mersenne Primes https://en.wikipedia.org/wiki/Mersenne_prime Mersenne prime is a prime number that is one less than a power of two. That is, it is a prime number of the form M_n = 2^n 1 for some integer n. They are named after Marin Mersenne, a French Minim friar, who studied them in the early 17th century. If n is a composite number then so is 2^n 1. Therefore, an equivalent definition of the Mersenne primes is that they are the prime numbers of the form M_p = 2^p 1 for some prime p.

QUESTION 2

What is a "Collision attack" in cryptography?

A. Collision attacks try to break the hash into three parts to get the plaintext value

B. Collision attacks try to get the public key

C. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key

D. Collision attacks try to find two inputs producing the same

Correct Answer: D

Collision attacks try to find two inputs producing the same https://en.wikipedia.org/wiki/Collision_attack

A collision attack on a cryptographic hash tries to find two inputs producing the same hash value, i.e. a hash collision. This is in contrast to a preimage attack where a specific target hash value is specified.

QUESTION 3

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 4

What type of encryption uses different keys to encrypt and decrypt the message?

A. Asymmetric

B. Symmetric

C. Secure

D. Private key

Correct Answer: A

Asymmetric https://en.wikipedia.org/wiki/Public-key_cryptography Asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys, which may be disseminated widely, and private keys, which are known only to the owner. The generation of such keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.

QUESTION 5

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

Correct Answer: C

RC4 https://en.wikipedia.org/wiki/RC4 RC4 (Rivest Cipher 4 also known as ARC4 or ARCFOUR meaning Alleged RC4, see below) is a stream cipher. While it is remarkable for its simplicity and speed in software, multiple vulnerabilities have been discovered in RC4, rendering it insecure. It is especially vulnerable when the beginning of the output keystream is not discarded, or when nonrandom or related keys are used. Particularly problematic uses of RC4 have led to very insecure protocols such as WEP. The key-scheduling algorithm is used to initialize the permutation in the array "S". "keylength" is defined as the number of bytes in the key and can be in the range 1 keylength 256, typically between 5

and 16, corresponding to a key length of 40 ?128 bits. First, the array "S" is initialized to the identity permutation. S is then processed for 256 iterations in a similar way to the main PRGA, but also mixes in bytes of the key at the same time.