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

Which of the following algorithms uses three different keys to encrypt the plain text?

A. Skipjack

B. AES

C. Blowfish

D. 3DES

Correct Answer: D

3DES https://en.wikipedia.org/wiki/Triple_DES Triple DES (3DES) has a three different keys with same size (56-bit).

QUESTION 2

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

Correct Answer: A

IV https://en.wikipedia.org/wiki/Initialization_vector In cryptography, an initialization vector (IV) or starting variable (SV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. For block ciphers, the use of an IV is described by the modes of operation. Randomization is also required for other primitives, such as universal hash functions and message authentication codes based thereon.

QUESTION 3

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

Correct Answer: A

Chosen plaintext https://en.wikipedia.org/wiki/Chosen-plaintext_attack A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker can obtain the ciphertexts for arbitrary plaintexts. The goal of the attack is to gain information that reduces the security of the encryption scheme.

QUESTION 4

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

Correct Answer: C

Any number only divisible by one and itself https://en.wikipedia.org/wiki/Prime_number A prime number (or a prime) is a natural number greater than 1 that is not a product of two smaller natural numbers. A natural number greater than 1 that is not prime is called a composite number. For example, 5 is prime because the only ways of writing it as a product, 1 ?5 or 5 ?1, involve 5 itself. However, 4 is composite because it is a product (2 ?2) in which both numbers are smaller than 4. Primes are central in number theory because of the fundamental theorem of arithmetic: every natural number greater than 1 is either a prime itself or can be factorized as a product of primes that is unique up to their order.

QUESTION 5

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)

Correct Answer: C

RA (Registration Authority)

https://en.wikipedia.org/wiki/Registration_authority Registration authorities exist for many standards organizations, such as ANNA (Association of National Numbering Agencies for ISIN), the Object Management Group, W3C, IEEE and others.

In general, registration authorities all perform a similar function, in promoting the use of a particular standard through facilitating its use. This may be by applying the standard, where appropriate, or by verifying that a particular application

satisfies the standard\\'s tenants. Maintenance agencies, in contrast, may change an element in a standard based on set rules ?such as the creation or change of a currency code when a currency is created or revalued (i.e. TRL to TRY for

Turkish lira). The Object Management Group has an additional concept of certified provider, which is deemed an entity permitted to perform some functions on behalf of the registration authority, under specific processes and procedures

documented within the standard for such a role.