



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.pass4itsure.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

The most widely used digital certificate standard. First issued July 3, 1988. It is a digital document that contains a public key signed by the trusted third party, which is known as a Certificate Authority, or CA. Relied on by S/MIME. Contains your name, info about you, and a signature of a person who issued the certificate.

A. ElGamal

B. RSA

C. PAP

D. X.509

Correct Answer: D

https://en.wikipedia.org/wiki/X.509 In cryptography, X.509 is a standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web. They are also used in offline applications, like electronic signatures. An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.

QUESTION 2

Which of the following encryption algorithms relies on the inability to factor large prime numbers?

A. RSA

B. MQV

C. EC

D. AES

Correct Answer: A

QUESTION 3

The art and science of writing hidden messages so that no one suspects the existence of the message, a type of security through obscurity. Message can be hidden in picture or audio file for example. Uses least significant bits in a file to store data.

- A. Steganography
- B. Cryptosystem
- C. Avalanche effect



D. Key Schedule

Correct Answer: A

Steganography

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

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages appear to be (or to be part of)

something else:

images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some implementations of steganography that lack a shared secret are forms of

security through obscurity, and key-dependent steganographic schemes adhere to Kerckhoffs\\'s principle.

QUESTION 4

A _____ refers to a situation where two different inputs yield the same output.

- A. Convergence
- B. Collision
- C. Transposition
- D. Substitution
- Correct Answer: B

Collision

https://en.wikipedia.org/wiki/Collision_(computer_science) A collision or clash is a situation that occurs when two distinct pieces of data have the same hash value, checksum, fingerprint, or cryptographic digest.

QUESTION 5

Original, unencrypted information is referred to as _____.

A. text

- B. plaintext
- C. ciphertext
- D. cleartext



Correct Answer: B

plaintext https://en.wikipedia.org/wiki/Plaintext In cryptography, plaintext usually means unencrypted information pending input into cryptographic algorithms, usually encryption algorithms. Cleartext usually refers to data that is transmitted or stored unencrypted ("in clear").

212-81 VCE Dumps

212-81 Study Guide

212-81 Braindumps