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

A. RSA

B. MQV

C. EC

D. AES

Correct Answer: A

QUESTION 2

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

Correct Answer: A

Public keys https://en.wikipedia.org/wiki/Public-key_cryptography Public-key cryptography, or 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. In such a system, any person can encrypt a message using the receiver\\'s public key, but that encrypted message can only be decrypted with the receiver\\'s private key.

Alice and Bob have two keys of their own -- just to be clear, that\\'s four keys total. Each party has their own public key, which they share with the world, and their own private key which they well, which they keep private, of course but, more than that, which they keep as a closely guarded secret. The magic of public key cryptography is that a message encrypted with the public key can only be decrypted with the private key. Alice will encrypt her message with Bob\\'s public key, and even though Eve knows she used Bob\\'s public key, and even though Eve knows Bob\\'s public key herself, she is unable to decrypt the message. Only Bob, using his secret key, can decrypt the message assuming he\\'s kept it secret, of course.

Alice and Bob do not need to plan anything ahead of time to communicate securely: they generate their public-private key pairs independently, and happily broadcast their public keys to the world at large. Alice can rest assured that only Bob can decrypt the message she sends because she has encrypted it with his public key.

QUESTION 3

Which of the following is a protocol for exchanging keys?

A. DH

B. EC

C. AES

D. RSA

Correct Answer: A

DH https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange Diffie-Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as conceived by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography. Published in 1976 by Diffie and Hellman, this is the earliest publicly known work that proposed the idea of a private key and a corresponding public key.

QUESTION 4

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.

QUESTION 5

WPA2 uses AES for wireless data encryption at which of the following encryption levels?

A. 128 bit and CRC

B. 128 bi and TKIP

C. 128 bit and CCMP

D. 64 bit and CCMP

Correct Answer: C

128 bit and CCMP

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol that forms part of the 802.11i standard for wireless local area networks (WLANs), particularly those using WiMax technology.

CCMP employs 128-bit keys and a 48-bit initialization vector that minimizes vulnerability to replay attacks.