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.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

QUESTION 1

Terrance oversees the key escrow server for his company. All employees use asymmetric cryptography to encrypt all emails. How many keys are needed for asymmetric cryptography?

A. 2

B. 4

C. 3

D. 1

Correct Answer: A

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.

QUESTION 2

The Clipper chip is notable in the history of cryptography for many reasons. First, it was designed for civilian used secure phones. Secondly, it was designed to use a very specific symmetric cipher. Which one of the following was originally designed to provide built-in cryptography for the Clipper chip?

A. Blowfish

B. Twofish

C. Skipjack

D. Serpent

Correct Answer: C

Skipjack https://en.wikipedia.org/wiki/Clipper_chip The Clipper chip was a chipset that was developed and promoted by the United States National Security Agency (NSA) as an encryption device that secured "voice and data messages" with a built-in backdoor that was intended to "allow Federal, State, and local law enforcement officials the ability to decode intercepted voice and data transmissions.". It was intended to be adopted by telecommunications companies for voice transmission. Introduced in 1993, it was entirely defunct by 1996. he Clipper chip used a data encryption algorithm called Skipjack to transmit information and the Diffie-Hellman key exchange-algorithm to distribute the cryptokeys between the peers. Skipjack was invented by the National Security Agency of the U.S. Government; this algorithm was initially classified SECRET, which prevented it from being subjected to peer review from the encryption research community. The government did state that it used an 80-bit key, that the algorithm was symmetric, and that it was similar to the DES algorithm. The Skipjack algorithm was declassified and published by the NSA on June 24, 1998. The initial cost of the chips was said to be $16 (unprogrammed) or $26 (programmed), with its logic designed by Mykotronx, and fabricated by VLSI Technology, Inc (see the VLSI logo on the image on this page).

QUESTION 3

What advantage do symmetric algorithms have over asymmetric algorithms

A. It is easier to implement them in software

B. They are more secure

C. They are faster

D. It is easier to exchange keys

Correct Answer: C

They are faster

Symmetric key encryption is much faster than asymmetric key encryption, because both the sender and the recipient of a message to use the same secret key.

QUESTION 4

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 5

What must occur in order for a cipher to be considered `broken\\'?

A. Uncovering the algorithm used

B. Decoding the key

C. Finding any method that is more efficient than brute force

D. Rendering the cipher no longer useable

Correct Answer: C

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."