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

You are studying classic ciphers. You have been examining the difference between single substitution and multi-substitution. Which one of the following is an example of a multi- alphabet cipher?

A. Rot13

B. Caesar

C. Atbash

D. Vigenere

Correct Answer: D

Vigenere https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher The Vigenere cipher is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It employs a form of polyalphabetic substitution. First described by Giovan Battista Bellaso in 1553, the cipher is easy to understand and implement, but it resisted all attempts to break it until 1863, three centuries later. This earned it the description le chiffre indehiffrable (French for \\'the indecipherable cipher\\'). Many people have tried to implement encryption schemes that are essentially Vigenre ciphers. In 1863, Friedrich Kasiski was the first to publish a general method of deciphering Vigenre ciphers.

QUESTION 2

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 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

Developed by Netscape and has been replaced by TLS. It was the preferred method used with secure websites.

A. OCSP

B. VPN

C. CRL

D. SSL

Correct Answer: D

SSL https://en.wikipedia.org/wiki/Transport_Layer_Security Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. Several versions of the protocols find widespread use in applications such as web browsing, email, instant messaging, and voice over IP (VoIP). Websites can use TLS to secure all communications between their servers and web browsers. Netscape developed the original SSL protocols, and Taher Elgamal, chief scientist at Netscape Communications from 1995 to 1998, has been described as the "father of SSL". SSL version 1.0 was never publicly released because of serious security flaws in the protocol. Version 2.0, released in February 1995, contained a number of security flaws which necessitated the design of version 3.0. Released in 1996, SSL version 3.0 represented a complete redesign of the protocol produced by Paul Kocher working with Netscape engineers Phil Karlton and Alan Freier, with a reference implementation by Christopher Allen and Tim Dierks of Consensus Development.

QUESTION 5

What does Output feedback (OFB) do:

A. The message is divided into blocks and each block is encrypted separately. This is the most basic mode for symmetric encryption

B. The cipher text from the current round is XORed with the plaintext from the previous round

C. A block cipher is converted into a stream cipher by generating a keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext

D. The cipher text from the current round is XORed with the plaintext for the next round

Correct Answer: C

A block cipher is converted into a stream cipher by generating a keystream blocks, which are then XORed with the

plaintext blocks to get the ciphertext
https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Output_feedback_(OFB) The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error-correcting codes to function normally even when applied before encryption.