100% Money Back Guarantee

Vendor:EC-COUNCIL

Exam Code:212-81

Exam Name:EC-Council Certified Encryption Specialist (ECES)

Version: Demo

QUESTION 1

Which of the following is a fundamental principle of cryptography that holds that the algorithm can be publicly disclosed without damaging security?

A. Vigenere\\'s principle

B. Shamir\\'s principle

C. Kerkchoff\\'s principle

D. Babbage\\'s principle

Correct Answer: C

Kerkchoff\\'s principle https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle Kerckhoffs\\'s principle (also called Kerckhoffs\\'s desideratum, assumption, axiom, doctrine or law) of cryptography was stated by Netherlands born cryptographer Auguste Kerckhoffs in the 19th century: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge. Kerckhoffs\\'s principle was reformulated (or possibly independently formulated) by American mathematician Claude Shannon as "the enemy knows the system", i.e., "one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them". In that form, it is called Shannon\\'s maxim. This concept is widely embraced by cryptographers, in contrast to "security through obscurity", which is not.

QUESTION 2

In relationship to hashing, the term _____refers to random bits that are used as one of the inputs to the hash. Essentially the _____ is intermixed with the message that is to be hashed

A. Vector

B. Salt

C. Stream

D. IV

Correct Answer: B

Salt

https://en.wikipedia.org/wiki/Salt_(cryptography)

A salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but

over time additional safeguards were developed to protect a user\\'s password against being read from the system. A salt is one of those methods.

QUESTION 3

If the round function is a cryptographically secure pseudorandom function, then ___rounds is sufficient to make it a "strong" pseudorandom permutation.

A. 15

B. 16

C. 3

D. 4

Correct Answer: D

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

Michael Luby and Charles Rackoff analyzed the Feistel cipher construction, and proved that if the round function is a cryptographically secure pseudorandom function, with Ki used as the seed, then 3 rounds are sufficient to make the block

cipher a pseudorandom permutation, while 4 rounds are sufficient to make it a "strong" pseudorandom permutation (which means that it remains pseudorandom even to an adversary who gets oracle access to its inverse permutation).

Because of this very important result of Luby and Rackoff, Feistel ciphers are sometimes called Luby-Rackoff block ciphers.

QUESTION 4

Jane is looking for an algorithm to ensure message integrity. Which of following would be an acceptable choice?

A. RSA

B. AES

C. RC4

D. SHA-1

Correct Answer: D

Integrity. In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner. An important application of hashes is verification of message integrity. Comparing message digests (hash digests over the message) calculated before, and after, transmission can determine whether any changes have been made to the message or file. SHA-1 https://en.wikipedia.org/wiki/SHA-1 SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest ?typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard.

QUESTION 5

Which of the following techniques is used (other than brute force) to attempt to derive a key?

A. Cryptography

B. Cryptoanalysis

C. Password cracking

D. Hacking

Correct Answer: B

Cryptoanalysis https://en.wikipedia.org/wiki/Cryptanalysis Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

QUESTION 6

What is the largest key size that AES can use?

A. 256

B. 56

C. 512

D. 128

Correct Answer: A

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

QUESTION 7

Electromechanical rotor-based cipher used in World War II

A. ROT13 Cipher

B. Cipher Disk

C. Enigma Machine

D. Rail Fence Cipher

Correct Answer: C

Enigma Machine https://en.wikipedia.org/wiki/Enigma_machine The Enigma machine is an encryption device developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication. It was employed extensively by Nazi Germany during World War II, in all branches of the German military. Enigma has an electromechanical rotor mechanism that scrambles the 26 letters of the alphabet.

QUESTION 8

This is a 128 bit hash that is specified by RFC 1321. It was designed by Ron Rivest in 1991 to replace an earlier hash

function.

A. SHA1

B. SHA-256

C. RSA

D. MD5

Correct Answer: D

MD5 https://en.wikipedia.org/wiki/MD5 The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database. MD5 was designed by Ronald Rivest in 1991 to replace an earlier hash function MD4, and was specified in 1992 as RFC 1321.

QUESTION 9

Cylinder tool. Wrap leather around to decode. The diameter is the key. Used in 7th century BC by greek poet Archilochus.

A. Cipher disk

B. Caesar cipher

C. Scytale

D. Enigma machine

Correct Answer: C

Scytale https://en.wikipedia.org/wiki/Scytale A scytale is a tool used to perform a transposition cipher, consisting of a cylinder with a strip of parchment wound around it on which is written a message. The ancient Greeks, and the Spartans in particular, are said to have used this cipher in 7th century BC to communicate during military campaigns. The recipient uses a rod of the same diameter on which the parchment is wrapped to read the message. It has the advantage of being fast and not prone to mistakes--a necessary property when on the battlefield. It can, however, be easily broken. Since the strip of parchment hints strongly at the method, the ciphertext would have to be transferred to something less suggestive, somewhat reducing the advantage noted.

QUESTION 10

The greatest weakness with symmetric algorithms is _____.

A. They are less secure than asymmetric

B. The problem of key exchange

C. The problem of generating keys

D. They are slower than asymmetric

Correct Answer: B

The problem of key exchange https://en.wikipedia.org/wiki/Symmetric-key_algorithm Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption (also known as asymmetric key encryption).

QUESTION 11

MD5 can best be described as which one of the following?

A. Asymmetric algorithm

B. Hashing algorithm

C. Digital signature

D. Symmetric algorithm

Correct Answer: B

Hashing algorithm https://en.wikipedia.org/wiki/MD5 The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database.

QUESTION 12

Which of the following was a multi alphabet cipher widely used from the 16th century to the early 20th century?

A. Atbash

B. Caesar

C. Scytale

D. Vigenere

Correct Answer: D