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

Ahlen is using a set of pre-calculated hashes to attempt to derive the passwords from a Windows SAM file. What is a set of pre-calculated hashes used to derive a hashed password called?

A. Hash matrix

B. Rainbow table

C. Password table

D. Hash table

Correct Answer: B

Rainbow table https://en.wikipedia.org/wiki/Rainbow_table A rainbow table is a precomputed table for caching the output of cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a key derivation function (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters. It is a practical example of a space-time tradeoff, using less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple key derivation function with one entry per hash. Use of a key derivation that employs a salt makes this attack infeasible.

QUESTION 2

Which of the following is the successor of SSL?

A. GRE

B. RSA

C. IPSec

D. TLS

Correct Answer: D

TLS

https://en.wikipedia.org/wiki/Transport_Layer_Security#History_and_development TLS 1.0 was first defined in RFC 2246 in January 1999 as an upgrade of SSL Version 3.0, and written by Christopher Allen and Tim Dierks of Consensus

Development. As stated in the RFC, "the differences between this protocol and SSL 3.0 are not dramatic, but they are significant enough to preclude interoperability between TLS 1.0 and SSL 3.0". Tim Dierks later wrote that these changes,

and the renaming from "SSL" to "TLS", were a face-saving gesture to Microsoft, "so it wouldn\\'t look [like] the IETF was just rubberstamping Netscape\\'s protocol".

QUESTION 3

The most widely used asymmetric encryption algorithm is what?

A. Vigenere

B. Caesar Cipher

C. RSA

D. DES

Correct Answer: C

RSA The RSA encryption algorithm is one of the most widely used public key encryption algorithms that have ever been invented. It was created by the three scientists Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977, and today it is increasingly being used in the network area.

QUESTION 4

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").

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.

QUESTION 6

Represents the total number of possible values of keys in a cryptographic algorithm or other security measure, such as a password.

A. Key Schedule

B. Key Clustering

C. Key Space

D. Key Exchange

Correct Answer: C

Key Space https://en.wikipedia.org/wiki/Key_space_(cryptography) Algorithm\\'s key space refers to the set of all possible permutations of a key. To prevent an adversary from using a brute-force attack to find the key used to encrypt a message, the key space is usually designed to be large enough to make such a search infeasible. On average, half the key space must be searched to find the solution. Another desirable attribute is that the key must be selected truly randomly from all possible key permutations. Should this not be the case, and the attacker is able to determine some factor that may influence how the key was selected, the search space (and hence also the search time) can be significantly reduced. Humans do not select passwords randomly, therefore attackers frequently try a dictionary attack before a brute force attack, as this approach can often produce the correct answer in far less time than a systematic brute force search of all possible character combinations.

QUESTION 7

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 8

Which one of the following best describes a process that splits the block of plaintext into two separate blocks, then applies the round function to one half, and finally swaps the two halves?

A. Block ciphers

B. Symmetric cryptography

C. Feistel cipher

D. Substitution cipher

Correct Answer: C

QUESTION 9

Basic information theory is the basis for modern symmetric ciphers. Understanding the terminology of information theory is, therefore, important. If a single change of a single bit in the plaintext causes changes in all the bits of the resulting ciphertext, what is this called?

A. Complete diffusion

B. Complete scrambling

C. Complete confusion

D. Complete avalanche

Correct Answer: D

QUESTION 10

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 11

What is Kerchoff\\'s principle?

A. A minimum of 15 rounds is needed for a Feistel cipher to be secure

B. Only the key needs to be secret, not the actual algorithm

C. Both algorithm and key should be kept secret

D. A minimum key size of 256 bits is necessary for security

Correct Answer: B

Only the key needs to be secret, not the actual algorithm https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle Kerckhoffs\\'s principle 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.

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

QUESTION 13

Which one of the following is an algorithm that uses variable length key from 1 to 256 bytes, which constitutes a state table that is used for subsequent generation of pseudorandom bytes and then a pseudorandom string of bits, which is XORed with the plaintext to produce the ciphertext?

A. PIKE

B. Twofish

C. RC4

D. Blowfish

Correct Answer: C

RC4 https://en.wikipedia.org/wiki/RC4 RC4 (Rivest Cipher 4 also known as ARC4 or ARCFOUR meaning Alleged RC4, see below) is a stream cipher. While it is remarkable for its simplicity and speed in software, multiple vulnerabilities have been discovered in RC4, rendering it insecure. It is especially vulnerable when the beginning of the output keystream is

not discarded, or when nonrandom or related keys are used. Particularly problematic uses of RC4 have led to very insecure protocols such as WEP. The key-scheduling algorithm is used to initialize the permutation in the array "S". "keylength" is defined as the number of bytes in the key and can be in the range 1 keylength 256, typically between 5 and 16, corresponding to a key length of 40 ?128 bits. First, the array "S" is initialized to the identity permutation. S is then processed for 256 iterations in a similar way to the main PRGA, but also mixes in bytes of the key at the same time.

QUESTION 14

Juanita has been assigned the task of selecting email encryption for the staff of the insurance company she works for. The various employees often use diverse email clients. Which of the following methods is available as an add-in for most email clients?

A. Caesar cipher

B. RSA

C. PGP

D. DES

Correct Answer: C

PGP https://en.wikipedia.org/wiki/Pretty_Good_Privacy Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. Phil Zimmermann developed PGP in 1991.

QUESTION 15

Hash algortihm created by the Russians. Produces a fixed length output of 256bits. Input message is broken up into 256 bit blocks. If block is less than 256 bits then it is padded with 0s.

A. TIGER

B. GOST

C. BEAR

D. FORK-256

Correct Answer: B

GOST https://en.wikipedia.org/wiki/GOST_(hash_function) The GOST hash function, defined in the standards GOST R 34.11-94 and GOST 34.311- 95 is a 256-bit cryptographic hash function. It was initially defined in the Russian national standard GOST R 34.11-94 Information Technology ?Cryptographic Information Security ?Hash Function. The equivalent standard used by other member-states of the CIS is GOST 34.311-95.