212-81$^{\text{Q\&As}}$

EC-Council Certified Encryption Specialist (ECES)

QUESTION 1

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 2

Uses a formula, M_n = 2^n 1 where n is a prime number, to generate primes. Works for 2, 3, 5, 7 but fails on 11 and on many other n values.

A. Fibonacci Numbers

B. Co-prime Numbers

C. Even Numbers

D. Mersenne Primes

Correct Answer: D

Correct answers: Mersenne Primes https://en.wikipedia.org/wiki/Mersenne_prime Mersenne prime is a prime number that is one less than a power of two. That is, it is a prime number of the form M_n = 2^n 1 for some integer n. They are named after Marin Mersenne, a French Minim friar, who studied them in the early 17th century. If n is a composite number then so is 2^n 1. Therefore, an equivalent definition of the Mersenne primes is that they are the prime numbers of the form M_p = 2^p 1 for some prime p.

QUESTION 3

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 4

A transposition cipher invented 1918 by Fritz Nebel, used a 36 letter alphabet and a modified Polybius square with a single columnar transposition.

A. ADFVGX Cipher

B. ROT13 Cipher

C. Book Ciphers

D. Cipher Disk

Correct Answer: A

ADFVGX Cipher https://en.wikipedia.org/wiki/ADFGVX_cipher ADFGVX cipher was a field cipher used by the German Army on the Western Front during World War I. ADFGVX was in fact an extension of an earlier cipher called ADFGX. Invented by Lieutenant Fritz Nebel (1891?977) and introduced in March 1918, the cipher was a fractionating transposition cipher which combined a modified Polybius square with a single columnar transposition.

QUESTION 5

A 160-bit hash algorithm developed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel for which there are 128, 256 and 320-bit versions is called what?

A. SHA1

B. MD5

C. FORK

D. RIPEMD

Correct Answer: D

RIPEMD https://en.wikipedia.org/wiki/RIPEMD RIPEMD (RIPE Message Digest) is a family of cryptographic hash functions developed in 1992 (the original RIPEMD) and 1996 (other variants). There are five functions in the family: RIPEMD, RIPEMD-128, RIPEMD-160, RIPEMD-256, and RIPEMD-320, of which RIPEMD-160 is the most common. The original RIPEMD, as well as RIPEMD-128, is not considered secure because 128-bit result is too small and also (for the original RIPEMD) because of design weaknesses. The 256- and 320-bit versions of RIPEMD provide the same level of security as RIPEMD-128 and RIPEMD-160, respectively; they are designed for applications where the security level is sufficient but longer hash result is necessary.

Latest 212-81 Dumps 212-81 VCE Dumps 212-81 Braindumps