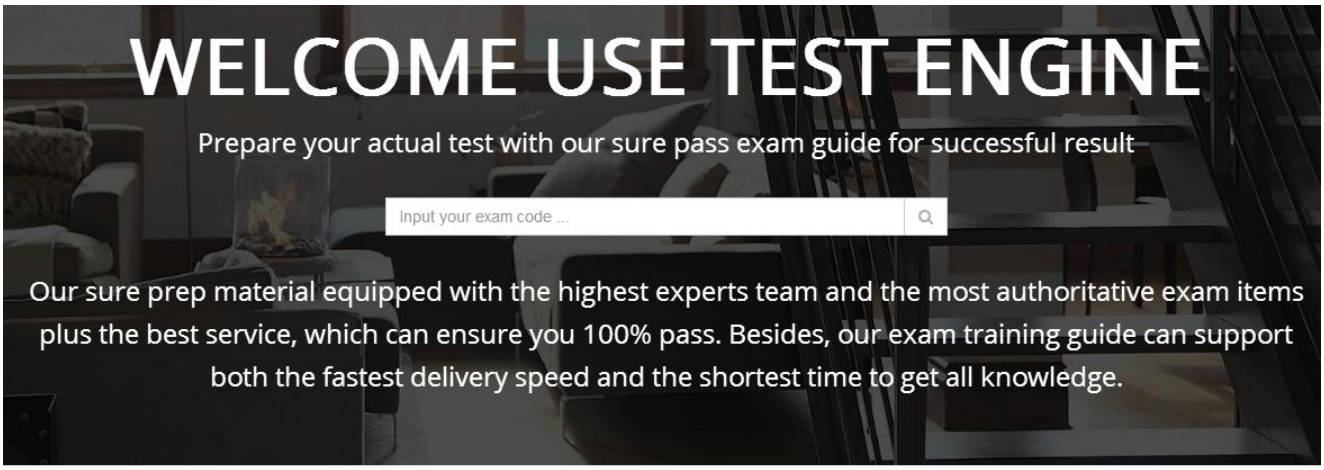
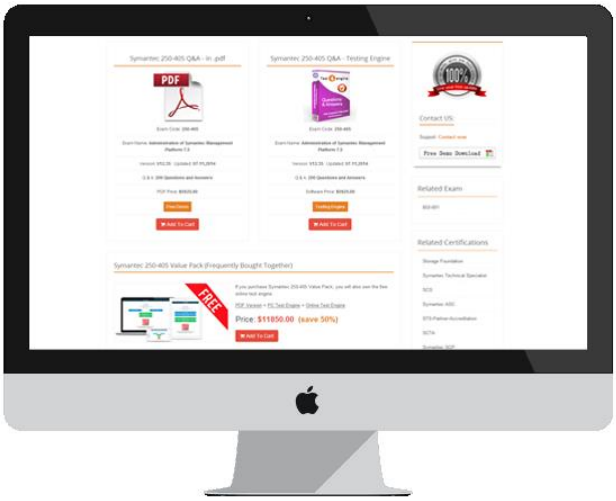
Prep4sureGuide

Prep4sureGuide





Quality and Value

Prep4sureGuide Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

Tested and Approved

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

Easy to Pass

If you prepare for the exams using our Prep4sureGuide testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

Try Before Buy

Prep4sureGuide offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

HAPPY CUSTOMERS	DOWNLOADS	TEAM MEMBERS	SHARES
32694	62152	32694	56692

http://www.prep4sureguide.com

Prepare your actual test with our sure pass exam guide for successful result

Exam : **212-81**

Title : Certified Encryption Specialist

Vendor : EC-COUNCIL

Version : DEMO

QUESTION NO: 1
A method for cracking modern cryptography. The attacker obtains the cipher texts corresponding to a set of plain texts of own choosing. Allows the attacker to attempt to derive the key. Difficult but not impossible.
A. Chosen Plaintext Attack
B. Steganography
C. Rainbow Tables
D. Transposition
Answer: A
Explanation:
Chosen Plaintext Attack
https://en.wikipedia.org/wiki/Chosen-plaintext_attack
A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker can obtain the ciphertexts for arbitrary plaintexts. The goal of the attack is to gain information that reduces the security of the encryption scheme.
Incorrect answers:
Rainbow Tables - precomputed table for caching the output of cryptographic hash functions, usually for cracking password hashes.
Transposition - swapping blocks of text.
Steganography - the practice of concealing a file, message, image, or video within another file, message, image, or video.

QUESTION NO: 2
What is a salt?
A. Key whitening
B. Random bits intermixed with a symmetric cipher to increase randomness and make it more secure
C. Key rotation
D. Random bits intermixed with a hash to increase randomness and reduce collisions
Answer: D
Explanation:
Random bits intermixed with a hash to increase randomness and reduce collisions
https://en.wikipedia.org/wiki/Salt_(cryptography)
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.
Incorrect answers:
Key whitening - a technique used to increase the security of block ciphers. It consists of steps that combine the data with portions of the key (most commonly using a simple XOR) before the first round and after the last round of encryption.
Key rotation - is when you retire an encryption key and replace that old key by generating a new cryptographic key. Rotating keys on a regular basis help meet industry standards and

cryptographic best practices.
Random bits intermixed with a symmetric cipher to increase randomness and make it more secure - Initialization Vector (IV)

QUESTION NO: 3
The next number is derived from adding together the prior two numbers (1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89).
A. Odd numbers
B. Fibonacci Sequence
C. Fermat pseudoprime
D. Prime numbers
Answer: B
Explanation:
Fibonacci Sequence
https://en.wikipedia.org/wiki/Fibonacci_number
In mathematics, the Fibonacci numbers, commonly denoted Fn, form a sequence, called the Fibonacci sequence, such that each number is the sum of the two preceding ones, starting from 0 and 1. That is, F0 = 0, F1=1, Fn = Fn-1 + Fn-2; for n > 1.
The beginning of the sequence is thus:
0,1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144...
Incorrect answers:
Prime numbers - numbers that have only 2 factors: 1 and themselves. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47...
Fermat numbers - a positive integer of the form Fn = 2^2^n +1; where n is a non-negative integer. The first few Fermat numbers are: 3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, ...
Odd numbers - any number which cannot be divided by two 1, 3, 5, 7, 9, 11, 13, 15 ...

QUESTION NO: 4
Encryption of the same plain text with the same key results in the same cipher text. Use of an IV that is XORed with the first block of plain text solves this problem.
A. CFB
B. GOST
C. ECB
D. RC4
Answer: C
Explanation:
ECB
https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
The simplest of the encryption modes is the electronic codebook (ECB) mode (named after conventional physical codebooks). The message is divided into blocks, and each block is encrypted separately.
The disadvantage of this method is a lack of diffusion. Because ECB encrypts identical plaintext blocks into identical ciphertext blocks, it does not hide data patterns well. ECB is not recommended for use in cryptographic protocols.

ECB mode can also make protocols without integrity protection even more susceptible to replay attacks, since each block gets decrypted in exactly the same way.
Incorrect answers:
RC4 - stream symmetric cipher that was created by Ron Rivest of RSA. Used in SSL and WEP.
GOST - the GOST block cipher (Magma), defined in the standard GOST 28147-89 (RFC 5830), is a Soviet and Russian government standard symmetric key block cipher with a block size of 64 bits. The original standard, published in 1989, did not give the cipher any name, but the most recent revision of the standard, GOST R 34.12-2015, specifies that it may be referred to as Magma. The GOST hash function is based on this cipher. The new standard also specifies a new 128-bit block cipher called Kuznyechik.
CFB - the process wherein the ciphertext block is encrypted then the ciphertext produced is XOR'd back with the plaintext to produce the current ciphertext block.

QUESTION NO: 5
If Bob is using asymmetric cryptography and wants to send a message to Alice so that only she can decrypt it, what key should he use to encrypt the message?
A. Alice's private key
B. Bob's private key
C. Alice's public key
D. Bob's public key
Answer: C
Explanation:
Alice's public key
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
In asymmetric (public key) cryptography, both communicating parties (i.e. both Alice and Bob) have two keys of their own - just to be clear, that's four keys total. Each party has their own public key, which they share with the world, and their own private key which they ... well, which they keep private, of course but, more than that, which they keep as a closely guarded secret. The magic of public key cryptography is that a message encrypted with the public key can only be decrypted with the private key. Alice will encrypt her message with Bob's public key, and even though Eve knows she used Bob's public key, and even though Eve knows Bob's public key herself, she is unable to decrypt the message. Only Bob, using his secret key, can decrypt the message ... assuming he's kept it secret, of course.

QUESTION NO: 6
A _____ is a function is not reversible.
A. Stream cipher
B. Asymmetric cipher
C. Hash
D. Block Cipher
Answer: C
Explanation:
Hash
https://en.wikipedia.org/wiki/Hash_function

Hash functions are irreversible. This is actually required for them to fulfill their function of determining whether someone possesses an uncorrupted copy of the hashed data. This brings susceptibility to brute force attacks, which are quite powerful these days, particularly against MD5.

QUESTION NO: 7
During the process of encryption and decryption, what keys are shared?
A. Public keys
B. Public and private keys
C. User passwords
D. Private keys
Answer: A
Explanation:
Public keys
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.
Alice and Bob have two keys of their own - just to be clear, that's four keys total. Each party has their own public key, which they share with the world, and their own private key which they well, which they keep private, of course but, more than that, which they keep as a closely guarded secret. The magic of public key cryptography is that a message encrypted with the public key can only be decrypted with the private key. Alice will encrypt her message with Bob's public key, and even though Eve knows she used Bob's public key, and even though Eve knows Bob's public key herself, she is unable to decrypt the message. Only Bob, using his secret key, can decrypt the message assuming he's kept it secret, of course.
Alice and Bob do not need to plan anything ahead of time to communicate securely: they generate their public-private key pairs independently, and happily broadcast their public keys to the world at large. Alice can rest assured that only Bob can decrypt the message she sends because she has encrypted it with his public key.

QUESTION NO: 8
What is the solution to the equation 8 mod 3?
A. 1
B. 4
C. 3
D. 2
Answer: D
Explanation:
2

https://en.wikipedia.org/wiki/Modulo_operation
The modulo operation returns the remainder or signed remainder of a division, after one number is divided by another (called the modulus of the operation).
Given two positive numbers a and n, a modulo n (abbreviated as a mod n) is the remainder of the Euclidean division of a by n, where a is the dividend and n is the divisor. The modulo operation is to be distinguished from the symbol mod, which refers to the modulus (or divisor) one is operating from.
For example, the expression "5 mod 2" would evaluate to 1, because 5 divided by 2 has a quotient of 2 and a remainder of 1, while "9 mod 3" would evaluate to 0, because the division of 9 by 3 has a quotient of 3 and a remainder of 0; there is nothing to subtract from 9 after multiplying 3 times 3.

QUESTION NO: 9
A _____ is a digital representation of information that identifies you as a relevant entity by a trusted third party.
A. Digital Signature
B. Hash
C. Ownership stamp
D. Digest
Answer: A
Explanation:
Digital Signature
https://en.wikipedia.org/wiki/Digital_signature
A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender (authentication), and that the message was not altered in transit (integrity).

QUESTION NO: 10
Calculates the average LSB and builds a table of frequencies and Pair of Values. Performs a test on the two tables. It measures the theoretical vs. calculated population difference.
A. Certificate Authority
B. Raw Quick Pair
C. Chi-Square Analysis
D. SP network
Answer: C
Explanation:
Chi-Square Analysis
https://en.wikipedia.org/wiki/Chi-squared_test
A chi-squared test, is a statistical hypothesis test that is valid to perform when the test statistic is chi-squared distributed under the null hypothesis, specifically Pearson's chi-squared test and variants thereof. Pearson's chi-squared test is used to determine whether there is a statistically significant difference between the expected frequencies and the observed frequencies in one or more categories of a contingency table.
In cryptanalysis, the chi-squared test is used to compare the distribution of plaintext and

(possibly) decrypted ciphertext. The lowest value of the test means that the decryption was successful with high probability. This method can be generalized for solving modern cryptographic problems.
Incorrect answers:
Raw Quick Pair - statistical analysis on number of unique colors and color number pairs in the picture and you look for least significant bits and manipulation of data in those bits, typically inside of whitespace.
SP network - substitution-permutation network is a series of linked mathematical operations used in block cipher algorithms such as AES (Rijndael), 3-Way, Kalyna, Kuznyechik, PRESENT, SAFER, SHARK, and Square.
Certificate Authority - component of a PKI that creates and maintains digital certificates throughout their life cycles.

QUESTION NO: 11
How can rainbow tables be defeated?
A. Lockout accounts under brute force password cracking attempts
B. All uppercase character passwords
C. Use of non-dictionary words
D. Password salting
Answer: D
Explanation:
Password salting
https://en.wikipedia.org/wiki/Salt_(cryptography)#Benefits
Salts also combat the use of hash tables and rainbow tables for cracking passwords. A hash table is a large list of pre-computed hashes for commonly used passwords. For a password file without salts, an attacker can go through each entry and look up the hashed password in the hash table or rainbow table. If the look-up is considerably faster than the hash function (which it often is), this will considerably speed up cracking the file. However, if the password file is salted, then the hash table or rainbow table would have to contain "salt . password" pre-hashed. If the salt is long enough and sufficiently random, this is very unlikely. Unsalted passwords chosen by humans tend to be vulnerable to dictionary attacks since they have to be both short and meaningful enough to be memorized. Even a small dictionary (or its hashed equivalent, a hash table) is significant help cracking the most commonly used passwords. Since salts do not have to be memorized by humans they can make the size of the rainbow table required for a successful attack prohibitively large without placing a burden on the users.

QUESTION NO: 12
Ciphers that write message letters out diagonally over a number of rows then read off cipher row by row. Also called zig-zag cipher.
A. Rail Fence Cipher
B. Null Cipher
C. Vigenere Cipher
D. ROT-13
Answer: A

Explanation:
Rail Fence Cipher
https://en.wikipedia.org/wiki/Rail_fence_cipher
The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded.
Incorrect answers:
Null cipher - also known as concealment cipher, is an ancient form of encryption where the plaintext is mixed with a large amount of non-cipher material. Today it is regarded as a simple form of steganography, which can be used to hide ciphertext.
Vigenère 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.
ROT13 - ("rotate by 13 places", sometimes hyphenated ROT-13) is a simple letter substitution cipher that replaces a letter with the 13th letter after it, in the alphabet. ROT13 is a special case of the Caesar cipher which was developed in ancient Rome.

QUESTION NO: 13
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
Answer: D
Explanation:
4
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 NO: 14
A _____ product refers to an NSA-endorsed classified or controlled cryptographic item for classified or sensitive U. S. government information, including cryptographic equipment, assembly, or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed
A. Type 1
B. Type 4
C. Type 2
D. Type 3
Answer: A

Explanation:
Type 1
https://en.wikipedia.org/wiki/NSA_cryptography#Type_1_Product
A Type 1 Product refers to an NSA endorsed classified or controlled cryptographic item for classified or sensitive U.S. government information, including cryptographic equipment, assembly or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed.
Incorrect answers:
Type 2 - product refers to an NSA endorsed unclassified cryptographic equipment, assemblies or components for sensitive but unclassified U.S. government information.
Type 3 - unclassified cryptographic equipment, assembly, or component used, when appropriately keyed, for encrypting or decrypting unclassified sensitive U.S. Government or commercial information, and to protect systems requiring protection mechanisms consistent with standard commercial practices. A Type 3 Algorithm refers to NIST endorsed algorithms, registered and FIPS published, for sensitive but unclassified U.S. government and commercial information.
Type 4 - Algorithm refers to algorithms that are registered by the NIST but are not FIPS published. Unevaluated commercial cryptographic equipment, assemblies, or components that are neither NSA nor NIST certified for any Government usage.

QUESTION NO: 15
Frank is trying to break into an encrypted file... He is attempting all the possible keys that could be used for this algorithm. Attempting to crack encryption by simply trying as many randomly generated keys as possible is referred to as what?
A. Rainbow table
B. Frequency analysis
C. Brute force
D. Kasiski
Answer: C
Explanation:
Brute force
https://en.wikipedia.org/wiki/Brute-force_attack
Brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.
Incorrect answers:
Kasiski - Kasiski examination (also referred to as Kasiski's test or Kasiski's method) is a method of attacking polyalphabetic substitution ciphers, such as the Vigenère cipher. It was first published by Friedrich Kasiski in 1863, but seems to have been independently discovered by Charles Babbage as early as 1846.
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.
Frequency analysis - (also known as counting letters) is the study of the frequency of letters or groups of letters in a ciphertext. The method is used as an aid to breaking classical ciphers.

QUESTION NO: 16
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
Answer: D
Explanation:
Vigenere
https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
The Vigenère 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 indéchiffrable (French for 'the indecipherable cipher'). Many people have tried to implement encryption schemes that are essentially Vigenère ciphers. In 1863, Friedrich Kasiski was the first to publish a general method of deciphering Vigenère ciphers.
Incorrect answers:
Caesar - Monoalphabetic cipher where letters are shifted one or more letters in either direction. The method is named after Julius Caesar, who used it in his private correspondence.
Atbash - Single substitution monoalphabetic cipher that substitutes each letter with its reverse (a and z, b and y, etc).
Scytale - Transposition cipher. A staff with papyrus or letter wrapped around it so edges would line up. There would be a stream of characters which would show you your message. When unwound it would be a random string of characters. Would need an identical size staff on other end for other individuals to decode message.

QUESTION NO: 17
Created by D. H. Lehmer. It is a classic example of a Linear congruential generator. A PRNG type of linear congruential generator (LCG) that operates in multiplicative group of integers modulo n. The basic algorithm is Xi+1=(aXi + c) mod m, with 0 ≤ Xi ≤ m.
A. Lehmer Random Number Generator
B. Lagged Fibonacci Generator
C. Linear Congruential Generator

D. Blum Blum Shub

Answer: A

Explanation:

Lehmer Random Number Generator

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

The Lehmer random number generator (named after D. H. Lehmer), sometimes also referred to as the Park-Miller random number generator (after Stephen K. Park and Keith W. Miller), is a type of linear congruential generator (LCG) that operates in multiplicative group of integers modulo n. The general formula is:

where the modulus m is a prime number or a power of a prime number, the multiplier a is an element of high multiplicative order modulo m (e.g., a primitive root modulo n), and the seed X0 is coprime to m.

Other names are multiplicative linear congruential generator (MLCG) and multiplicative congruential generator (MCG).

QUESTION NO: 18

Which of the following is an asymmetric algorithm related to the equation y^2 = x^3 + Ax + B?

A. Blowfish

B. Elliptic Curve

C. AES

D. RSA

Answer: B

Explanation:

Elliptic Curve

https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

For current cryptographic purposes, an elliptic curve is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation:

QUESTION NO: 19

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

Answer: B

Explanation:

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 NO: 20

How many qubits are needed to break RSA?

A. 1000
B. 2000
C. 4000
D. 100
Answer: C

QUESTION NO: 21
Algorithm that was chosen for the Data Encryption Standard, which was altered and renamed Data Encryption Algorithm.
A. Blowfish
B. Rijndael
C. Lucifer
D. El Gamal
Answer: C
Explanation:
Lucifer
https://en.wikipedia.org/wiki/Lucifer_(cipher)
Lucifer was a direct precursor to the Data Encryption Standard. One version, alternatively named DTD-1.