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.passapply.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

Which of the following is generally true about key sizes?

A. Larger key sizes increase security

B. Key size is irrelevant to security

C. Key sizes must be more than 256 bits to be secure

D. Smaller key sizes increase security

Correct Answer: A

Larger key sizes increase security https://en.wikipedia.org/wiki/Key_size Key length defines the upper-bound on an algorithm\\'s security (i.e. a logarithmic measure of the fastest known attack against an algorithm), since the security of all algorithms can be violated by brute-force attacks. Ideally, the lower-bound on an algorithm\\'s security is by design equal to the key length (that is, the security is determined entirely by the keylength, or in other words, the algorithm\\'s design doesn\\'t detract from the degree of security inherent in the key length). Indeed, most symmetric-key algorithms are designed to have security equal to their key length. However, after design, a new attack might be discovered. For instance, Triple DES was designed to have a 168 bit key, but an attack of complexity 2112 is now known (i.e. Triple DES now only has 112 bits of security, and of the 168 bits in the key the attack has rendered 56 \\'ineffective\\' towards security). Nevertheless, as long as the security (understood as \\'the amount of effort it would take to gain access\\') is sufficient for a particular application, then it doesn\\'t matter if key length and security coincide. This is important for asymmetric-key algorithms, because no such algorithm is known to satisfy this property; elliptic curve cryptography comes the closest with an effective security of roughly half its key length.

QUESTION 2

Which of the following is assured by the use of a hash?

A. Confidentiality

B. Availability

C. Authentication

D. Integrity

Correct Answer: D

Integrity https://en.wikipedia.org/wiki/Cryptographic_hash_function#Verifying_the_integrity_of_mess ages_and_files An important application of secure 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.

QUESTION 3

A cryptanalysis success where the attacker deduces the secret key.

A. Information Deduction

B. Avalanche effect

C. Shannon\\'s Entropy

D. Total Break

Correct Answer: D

Total Break

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

The results of cryptanalysis can also vary in usefulness. For example, cryptographer Lars Knudsen (1998) classified various types of attack on block ciphers according to the amount and quality of secret information that was discovered:

Total break -- the attacker deduces the secret key. Global deduction -- the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key. Instance (local) deduction -- the attacker discovers

additional plaintexts (or ciphertexts) not previously known.

Information deduction -- the attacker gains some Shannon information about plaintexts (or ciphertexts) not previously known.

Distinguishing algorithm -- the attacker can distinguish the cipher from a random permutation.

QUESTION 4

Numbers that have no factors in common with another.

A. Fibonacci Numbers

B. Even Numbers

C. Co-prime numbers

D. Mersenne Primes

Correct Answer: C

Correct answers: Co-prime numbers https://en.wikipedia.org/wiki/Coprime_integers Two integers a and b are said to be relatively prime, mutually prime, or coprime if the only positive integer (factor) that evenly divides both of them is 1. Consequently, any prime number that divides one of a or b does not divide the other. This is equivalent to their greatest common divisor (gcd) being 1. The numerator and denominator of a reduced fraction are coprime. The numbers 14 and 25 are coprime, since 1 is their only common divisor. On the other hand, 14 and 21 are not coprime, because they are both divisible by 7.

QUESTION 5

In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known as wardriving.

Which Algorithm is this referring to?

A. Wired Equivalent Privacy (WEP)

B. Wi-Fi Protected Access 2 (WPA2)

C. Wi-Fi Protected Access (WPA)

D. Temporal Key Integrity Protocol (TKIP)

Correct Answer: A

Wired Equivalent Privacy (WEP) https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy#Weak_security In 2007, Erik Tews, Andrei Pychkine, and Ralf-Philipp Weinmann were able to extend Klein\\'s 2005 attack and optimize it for usage against WEP. With the new attack it is possible to recover a 104-bit WEP key with probability 50% using only 40,000 captured packets. For 60,000 available data packets, the success probability is about 80% and for 85,000 data packets about 95%. Using active techniques like deauth and ARP re-injection, 40,000 packets can be captured in less than one minute under good conditions. The actual computation takes about 3 seconds and 3 MB of main memory on a Pentium-M 1.7 GHz and can additionally be optimized for devices with slower CPUs. The same attack can be used for 40-bit keys with an even higher success probability.