212-81 Q&As

EC-Council Certified Encryption Specialist (ECES)

QUESTION 1

What type of encryption uses different keys to encrypt and decrypt the message?

A. Asymmetric

B. Symmetric

C. Secure

D. Private key

Correct Answer: A

Asymmetric https://en.wikipedia.org/wiki/Public-key_cryptography 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.

QUESTION 2

Which service in a PKI will vouch for the identity of an individual or company?

A. CA

B. CR

C. KDC

D. CBC

Correct Answer: A

CA

https://en.wikipedia.org/wiki/Certificate_authority A certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.

This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party--trusted both by the subject (owner) of the certificate and by

the party relying upon the certificate. The format of these certificates is specified by the X.509 or EMV standard.

QUESTION 3

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 4

A linear congruential generator is an example of what?

A. A coprime generator

B. A prime number generator

C. A pseudo random number generator

D. A random number generator

Correct Answer: C

A pseudo random number generator https://en.wikipedia.org/wiki/Linear_congruential_generator A linear congruential generator (LCG) is an algorithm that yields a sequence of pseudo- randomized numbers calculated with a discontinuous piecewise linear equation. The method represents one of the oldest and best-known pseudorandom number generator algorithms. The theory behind them is relatively easy to understand, and they are easily implemented and fast, especially on computer hardware which can provide modular arithmetic by storage-bit truncation.

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.