# 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.leads4pass.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**

Ferris has been assigned the task of selecting security for his company\\'s wireless network. It is important that he pick the strongest form of wireless security. Which one of the following is the strongest wireless security?

A. WEP

B. WPA

C. WPA2

D. TKIP

Correct Answer: C

WPA2 https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access WPA (sometimes referred to as the draft IEEE 802.11i standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2, which became available in 2004 and is a common shorthand for the full IEEE 802.11i (or IEEE 802.11i-2004) standard.

**QUESTION 2**

If you wished to see a list of revoked certificates from a CA, where would you look?

A. RA

B. RFC

C. CRL

D. CA

Correct Answer: C

CRL https://ru.wikipedia.org/wiki/Certificate_Revocation_List Certificate Revocation List (or CRL) is "a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date and should no longer be trusted".

**QUESTION 3**

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

Correct Answer: D

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.

---

**QUESTION 4**

Manipulating individuals so that they will divulge confidential information, rather than by breaking in or using technical cracking techniques.

A. Linear cryptanalysis

B. Replay attack

C. Side-channel attack

D. Social engineering attack

Correct Answer: D

Social engineering attack https://en.wikipedia.org/wiki/Social_engineering_(security) Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. This differs from social engineering within the social sciences, which does not concern the divulging of confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

---

**QUESTION 5**

Jane is looking for an algorithm to ensure message integrity. Which of following would be an acceptable choice?

A. RSA

B. AES

C. RC4

D. SHA-1

Correct Answer: D

Integrity. In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner. An important application of 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. SHA-1 https://en.wikipedia.org/wiki/SHA-1 SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest ?typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard.

[212-81 PDF Dumps](#) [212-81 VCE Dumps](#) [212-81 Study Guide](#)