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 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

Which one of the following is an authentication method that sends the username and password in cleartext?

A. PAP

B. CHAP

C. Kerberos

D. SPAP

Correct Answer: A

PAP https://en.wikipedia.org/wiki/Password_Authentication_Protocol Password Authentication Protocol (PAP) is a password-based authentication protocol used by Point to Point Protocol (PPP) to validate users. Almost all network operating system remote servers support PAP. PAP is specified in RFC 1334. PAP is considered a weak authentication scheme (weak schemes are simple and have lighter computational overhead but are much more vulnerable to attack; while weak schemes may have limited application in some constrained environments, they are avoided in general). Among PAP\\'s deficiencies is the fact that it transmits unencrypted passwords (i.e. in plain-text) over the network. PAP is therefore used only as a last resort when the remote server does not support a stronger scheme such as CHAP or EAP.

QUESTION 3

This is a 128 bit hash that is specified by RFC 1321. It was designed by Ron Rivest in 1991 to replace an earlier hash function.

A. SHA1

B. SHA-256

C. RSA

D. MD5

Correct Answer: D

MD5 https://en.wikipedia.org/wiki/MD5 The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database. MD5 was designed by Ronald Rivest in 1991 to replace an earlier hash function MD4, and was specified in 1992 as RFC 1321.

QUESTION 4

Which algorithm was U. S. Patent 5,231,668, filed on july 26, 1991, attributed to David W. Kravitz, and adopted by the U. S. government in 1993 with FIPS 186?

A. DSA

B. AES

C. RC4

D. RSA

Correct Answer: A

DSA https://en.wikipedia.org/wiki/Digital_Signature_Algorithm DSA is covered by U.S. Patent 5,231,668 , filed July 26, 1991 and now expired, and attributed to David W. Kravitz, a former NSA employee. This patent was given to "The United States of America as represented by the Secretary of Commerce, Washington, D.C.", and NIST has made this patent available worldwide royalty-free. Claus P. Schnorr claims that his U.S. Patent 4,995,082 (also now expired) covered DSA; this claim is disputed.

QUESTION 5

Which one of the following is an example of a symmetric key algorithm?

A. ECC

B. Diffie-Hellman

C. RSA

D. Rijndael

Correct Answer: D

Rijndael https://en.wikipedia.org/wiki/Advanced_Encryption_Standard The Advanced Encryption Standard (AES), also known by its original name Rijndael. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.