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.pass4itsure.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

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

What must occur in order for a cipher to be considered `broken\\'?

A. Uncovering the algorithm used

B. Decoding the key

C. Finding any method that is more efficient than brute force

D. Rendering the cipher no longer useable

Correct Answer: C

Finding any method that is more efficient than brute force https://en.wikipedia.org/wiki/Cryptanalysis

Bruce Schneier notes that even computationally impractical attacks can be considered breaks: "Breaking a cipher simply means finding a weakness in the cipher that can be exploited with a complexity less than brute force."

QUESTION 2

Which of the following acts as a verifier for the certificate authority?

A. Certificate Management system

B. Directory management system

C. Registration authority

D. Certificate authority

Correct Answer: C

Registration authority https://en.wikipedia.org/wiki/Registration_authority Registration authorities exist for many standards organizations, such as ANNA (Association of National Numbering Agencies for ISIN), the Object Management Group, W3C, IEEE and others. In general, registration authorities all perform a similar function, in promoting the use of a particular standard through facilitating its use. This may be by applying the standard, where appropriate, or by verifying that a particular application satisfies the standard\\'s tenants. Maintenance agencies, in contrast, may change an element in a standard based on set rules ?such as the creation or change of a currency code when a currency is created or revalued (i.e. TRL to TRY for Turkish lira). The Object Management Group has an additional concept of certified provider, which is deemed an entity permitted to perform some functions on behalf of the registration authority, under specific processes and procedures documented within the standard for such a role.

QUESTION 3

RFC 1321 describes what hash?

A. RIPEMD

B. GOST

C. SHA1

D. MD5

Correct Answer: D

MD5 https://en.wikipedia.org/wiki/MD5 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 one of the following uses three different keys, all of the same size?

A. 3DES

B. AES

C. RSA

D. DES

Correct Answer: A

3DES https://en.wikipedia.org/wiki/Triple_DES Triple DES (3DES or TDES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block.

QUESTION 5

Cylinder tool. Wrap leather around to decode. The diameter is the key. Used in 7th century BC by greek poet Archilochus.

A. Cipher disk

B. Caesar cipher

C. Scytale

D. Enigma machine

Correct Answer: C

Scytale https://en.wikipedia.org/wiki/Scytale A scytale is a tool used to perform a transposition cipher, consisting of a cylinder with a strip of parchment wound around it on which is written a message. The ancient Greeks, and the Spartans in particular, are said to have used this cipher in 7th century BC to communicate during military campaigns. The recipient uses a rod of the same diameter on which the parchment is wrapped to read the message. It has the advantage of being fast and not prone to mistakes--a necessary property when on the battlefield. It can, however, be easily broken. Since the strip of parchment hints strongly at the method, the ciphertext would have to be transferred to something less suggestive, somewhat reducing the advantage noted.

212-81 VCE Dumps 212-81 Study Guide 212-81 Exam Questions