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

QUESTION 1

The ATBASH cipher is best described as what type of cipher?

A. Asymmetric

B. Symmetric

C. Substitution D. Transposition

Correct Answer: C

Substitution https://en.wikipedia.org/wiki/Atbash Atbash is a monoalphabetic substitution cipher originally used to encrypt the Hebrew alphabet. It can be modified for use with any known writing system with a standard collating order.

QUESTION 2

Algorithm that was chosen for the Data Encryption Standard, which was altered and renamed Data Encryption Algorithm.

A. Blowfish

B. Rijndael

C. Lucifer

D. El Gamal

Correct Answer: C

Lucifer

https://en.wikipedia.org/wiki/Lucifer_(cipher)

Lucifer was a direct precursor to the Data Encryption Standard. One version, alternatively named DTD-1.

QUESTION 3

In a Feistel cipher, the two halves of the block are swapped in each round. What does this provide?

A. Diffusion

B. Confusion

C. Avalanche

D. Substitution

Correct Answer: B

Confusion https://en.wikipedia.org/wiki/Confusion_and_diffusion#Definition Confusion means that each binary digit (bit)

of the ciphertext should depend on several parts of the key, obscuring the connections between the two. The property of confusion hides the relationship between the ciphertext and the key. This property makes it difficult to find the key from the ciphertext and if a single bit in a key is changed, the calculation of the values of most or all of the bits in the ciphertext will be affected. Confusion increases the ambiguity of ciphertext and it is used by both block and stream ciphers.

Incorrect answer: Avalanche - The avalanche effect is the desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions, wherein if an input is changed slightly (for example, flipping a single bit), the output changes significantly (e.g., half the output bits flip). In the case of high-quality block ciphers, such a small change in either the key or the plaintext should cause a drastic change in the ciphertext. The actual term was first used by Horst Feistel, although the concept dates back to at least Shannon\\'s diffusion. Diffusion - Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change.[2] Since a bit can have only two states, when they are all re-evaluated and changed from one seemingly random position to another, half of the bits will have changed state. Substitution - Substitution technique is a classical encryption technique where the characters present in the original message are replaced by the other characters or numbers or by symbols.

QUESTION 4

This hash function uses 512-bit blocks and implements preset constants that change after each repetition. Each block is hashed into a 256-bit block through four branches that divides each 512 block into sixteen 32-bit words that are further encrypted and rearranged.

A. SHA-256

B. FORK-256

C. SHA-1

D. RSA

Correct Answer: B

FORK-256 https://en.wikipedia.org/wiki/FORK-256 FORK-256 was introduced at the 2005 NIST Hash workshop and published the following year.[6] FORK-256 uses 512-bit blocks and implements preset constants that change after each repetition. Each block is hashed into a 256-bit block through four branches that divides each 512 block into sixteen 32-bit words that are further encrypted and rearranged.

QUESTION 5

Created in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT. Most widely used public key cryptography algorithm. Based on relationships with prime numbers. This algorithm is secure because it is difficult to factor a large integer composed of two or more large prime factors.

A. PKI

B. DES

C. RSA

D. Diffie-Helmann

Correct Answer: C

RSA

https://en.wikipedia.org/wiki/RSA_(cryptosystem)

RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who

publicly described the algorithm in 1977. An equivalent system was developed secretly, in 1973 at GCHQ (the British signals intelligence agency), by the English mathematician Clifford Cocks. That system was declassified in 1997.