KaozhengPro

# IT認證考試題庫

# 專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

**Exam** : **212-81**

**Title** : EC-Council Certified Encryption Specialist (ECES)

**Version** : DEMO

1.What size block does AES work on?
A. 64
B. 128
C. 192
D. 256
**Answer:** B
**Explanation:**
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

2.Which of the following is a type of encryption that has two different keys. One key can encrypt the message and the other key can only decrypt it?
A. Block cipher
B. Asymmetric
C. Symmetric
D. Stream cipher
**Answer:** B
**Explanation:**
Asymmetric
Public-key cryptography, or 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.

3.The reverse process from encoding - converting the encoded message back into its plaintext format.
A. Substitution
B. Whitening
C. Encoding
D. Decoding
**Answer:** D
**Explanation:**
Decoding
Decoding - reverse process from encoding,converting the encoded message back into its plaintext format.

4.Which of the following are valid key sizes for AES (choose three)?
A. 192
B. 56
C. 256
D. 128
E. 512

F. 64

**Answer:** A,C,D

**Explanation:**

Correct answers: 128, 192, 256 https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

The Advanced Encryption Standard (AES), also known by its original name Rijndael, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

5.A non-secret binary vector used as the initializing input algorithm for encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance.

A. IV

B. Salt

C. L2TP

D. Nonce

**Answer:** A

**Explanation:**

IV

https://en.wikipedia.org/wiki/Initialization_vector

In cryptography, an initialization vector (IV) or starting variable (SV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. For block ciphers, the use of an IV is described by the modes of operation. Randomization is also required for other primitives, such as universal hash functions and message authentication codes based thereon.