
**Vendor:**EC-COUNCIL

**Exam Code:**212-81

**Exam Name:**EC-Council Certified Encryption Specialist (ECES)

**Version:**Demo

**QUESTION 1**

John works as a cryptography consultant. He finds that people often misunderstand the reality of breaking a cipher. What is the definition of breaking a cipher?

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

B. Uncovering the algorithm used

C. Rendering the cypher no longer useable

D. Decoding the key

Correct Answer: A

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. Never mind that

brute-force might require 2^128 encryptions; an attack requiring 2^110 encryptions would be considered a break...simply put, a break can just be a certificational weakness: evidence that the cipher does not perform as advertised."

---

**QUESTION 2**

With Cipher feedback (CFB) what happens?

A. The key is reapplied

B. The ciphertext block is encrypted then the ciphertext produced is XOR\\'d back with the plaintext to produce the current ciphertext block

C. The block cipher is turned into a stream cipher

D. The message is divided into blocks and each block is encrypted separately. This is the most basic mode for symmetric encryption

Correct Answer: B

The ciphertext block is encrypted then the ciphertext produced is XOR\\'d back with the plaintext to produce the current ciphertext block https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Cipher_feedback_(CFB) The cipher feedback (CFB) mode, a close relative of CBC, makes a block cipher into a self- synchronizing stream cipher.

---

**QUESTION 3**

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 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

Correct Answer: ACD

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.

---

**QUESTION 5**

A simple algorithm that will take the initial key and from that generate a slightly different key each round.

A. Key Schedule

B. Feistel Network

C. SHA-2

D. Diffie-Helman

Correct Answer: A

Key Schedule https://en.wikipedia.org/wiki/Key_schedule In cryptography, the so-called product ciphers are a certain kind of cipher, where the (de- )ciphering of data is typically done as an iteration of rounds. The setup for each round is

generally the same, except for round-specific fixed values called a round constant, and round-specific data derived from the cipher key called a round key. A key schedule is an algorithm that calculates all the round keys from the key.

---

**QUESTION 6**

The greatest weakness with symmetric algorithms is _____.

A. They are less secure than asymmetric

B. The problem of key exchange

C. The problem of generating keys

D. They are slower than asymmetric

Correct Answer: B

The problem of key exchange https://en.wikipedia.org/wiki/Symmetric-key_algorithm Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption (also known as asymmetric key encryption).

---

**QUESTION 7**

A type of frequency analysis used to attack polyalphabetic substitution ciphers. It\\'s used to try to discover patterns and use that information to decrypt the cipher.

A. Kasiski Method

B. Birthday Attack

C. Information Deduction

D. Integral Cryptanalysis

Correct Answer: A

Kasiski Method https://en.wikipedia.org/wiki/Kasiski_examination In cryptanalysis, Kasiski examination (also referred to as Kasiski\\'s test or Kasiski\\'s method) is a method of attacking polyalphabetic substitution ciphers, such as the Vigen?e cipher. It was first published by Friedrich Kasiski in 1863, but seems to have been independently discovered by Charles Babbage as early as 1846.

---

**QUESTION 8**

A cryptanalysis success where the attacker deduces the secret key.

A. Information Deduction

B. Avalanche effect

C. Shannon\\'s Entropy

D. Total Break

Correct Answer: D

Total Break

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

The results of cryptanalysis can also vary in usefulness. For example, cryptographer Lars Knudsen (1998) classified various types of attack on block ciphers according to the amount and quality of secret information that was discovered:

Total break -- the attacker deduces the secret key. Global deduction -- the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key. Instance (local) deduction -- the attacker discovers

additional plaintexts (or ciphertexts) not previously known.

Information deduction -- the attacker gains some Shannon information about plaintexts (or ciphertexts) not previously known.

Distinguishing algorithm -- the attacker can distinguish the cipher from a random permutation.

---

**QUESTION 9**

Which of the following is an asymmetric algorithm related to the equation y^2 = x^3 + Ax + B?

A. Blowfish

B. Elliptic Curve

C. AES

D. RSA

Correct Answer: B

Elliptic Curve

https://en.wikipedia.org/wiki/Elliptic-curve_cryptography For current cryptographic purposes, an elliptic curve is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation:

---

**QUESTION 10**

Basic information theory is the basis for modern symmetric ciphers. Understanding the terminology of information theory is, therefore, important. If a single change of a single bit in the plaintext causes changes in all the bits of the resulting ciphertext, what is this called?

A. Complete diffusion

B. Complete scrambling

C. Complete confusion

D. Complete avalanche

Correct Answer: D

---

**QUESTION 11**

What is the formula m^e %n related to?

A. Encrypting with EC

B. Decrypting with RSA

C. Generating Mersenne primes

D. Encrypting with RSA

Correct Answer: D

Encrypting with RSA

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

RSA Encrypting a message m (number) with the public key (n, e) is calculated:

M\\' := m^e %n

---

**QUESTION 12**

Developed by Netscape and has been replaced by TLS. It was the preferred method used with secure websites.

A. OCSP

B. VPN

C. CRL

D. SSL

Correct Answer: D

SSL https://en.wikipedia.org/wiki/Transport_Layer_Security Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. Several versions of the protocols find widespread use in applications such as web browsing, email, instant messaging, and voice over IP (VoIP). Websites can use TLS to secure all communications between their servers and web browsers. Netscape developed the original SSL protocols, and Taher Elgamal, chief scientist at Netscape Communications from 1995 to 1998, has been described as the "father of SSL". SSL version 1.0 was never publicly released because of serious security flaws in the protocol. Version 2.0, released in February 1995, contained a number of security flaws which necessitated the design of version 3.0. Released in 1996, SSL version 3.0 represented a complete redesign of the protocol produced by Paul Kocher working with Netscape engineers Phil Karlton and Alan Freier, with a reference implementation by Christopher Allen and Tim Dierks of Consensus Development.