Question #1 *Topic 1*

3DES can best be classified as which one of the following?

A. Hashing algorithm

B. Digital signature

C. Symmetric algorithm

D. Asymmetric algorithm

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

You have been tasked with selecting a digital certificate standard for your company to use. Which one of the following is an international standard for the format and information contained in a digital certificate?

A. CA

B. CRL

C. RFC 2298

D. X.509

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

What is the basis for the difficulty in breaking RSA?

A. Factoring numbers

B. Hashing

C. Equations that describe an elliptic curve

D. The birthday paradox

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #4 Topic 1

How does Kerberos generate the first secret key in the authentication process?

A. By creating a hash of the user password

B. By generating a random AES key

C. By using the user's public key

D. By hashing the user ID, network ID, and salt

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #5

Topic 1

The mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext.

A. Electronic codebook (ECB)

B. Output feedback (OFB)

C. Cipher feedback (CFB)

D. Cipher block chaining (CBC)

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #6

Topic 1

Ferris has been assigned the task of selecting security for his company’s wireless network. It is important that he pick the strongest form of wireless security. Which one of the following is the strongest wireless security?

A. WEP

B. TKIP

C. WPA2

D. WPA

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

Tom is explaining historical cryptography to a class of security students. Which of the following ciphers is a subset of the Vigenère cipher?

A. Scytale

B. Caesar

C. Blowfish

D. Atbash

Suggested Answer: *C*

Community vote distribution

B (100%)

m36 9 months ago

Selected Answer: B

The Caesar cipher is a subset of the Vigenère cipher.

Scytale is a transposition cipher, not a substitution cipher like the Vigenère.

Blowfish is a modern block cipher, unrelated to the Vigenère cipher.

Atbash is a substitution cipher where the alphabet is reversed (i.e., 'A' becomes 'Z', 'B' becomes 'Y', etc.), not a Vigenère cipher variant.

upvoted 1 times

Question #8 *Topic 1*

What is a variation of DES that uses a technique called Key Whitening?

A. AES

B. 3DES

C. DESX

D. Blowfish

Suggested Answer: *C*

Community vote distribution

C (100%)

m36 9 months ago

Selected Answer: C

DESX is a variation of the DES that uses a technique called key whitening.

AES (Advanced Encryption Standard) is a modern encryption algorithm and is not a variant of DES, nor does it use key whitening.
3DES (Triple DES) applies DES three times with different keys, but it does not involve key whitening.
Blowfish is a separate symmetric-key block cipher and is not related to DES or key whitening.

upvoted 1 times

Question #9 *Topic 1*

While many companies are working on quantum computing, what is the current biggest challenge?

A. Processing speed

B. Decoherence

C. Funding

D. Power needs

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Which of the following techniques is used (other than brute force) to attempt to derive a key?

A. Password cracking

B. Cryptography

C. Hacking

D. Cryptanalysis

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Juanita has been assigned the task of selecting email encryption for the staff of the insurance company she works for. The various employees often use diverse email clients. Which of the following methods is available as an add-in for most email clients?

A. Caesar cipher

B. DES

C. RSA

D. PGP

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

What is the name of the attack where the attacker obtains the ciphertexts corresponding to a set of plaintexts of his own choosing?

A. Kasisiki examination

B. Known plaintext

C. Differential analysis

D. Chosen plaintext

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 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. Rendering the cipher no longer usable

C. Uncovering the algorithm used

D. Decoding the key

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #14 Topic 1

In order to understand RSA, you must understand the key generation algorithm as well as the encryption and decryption algorithms. Which one of the following equations describes the encryption process for RSA?

A. P = Cd mod n

B. Ce mod n

C. y2 = x3+Ax+B

D. Me mod n

Suggested Answer: *D*

Community vote distribution

D (100%)

lykbay 3 months, 3 weeks ago

Selected Answer: D

The RSA encryption process is described by the following mathematical equation:

C
=
M
e
m
o
d

n
C=M
e
modn

Where:

C
C is the ciphertext (the encrypted message),

M
M is the plaintext (the original message),

e
e is the public exponent,

n
n is the modulus (part of the public key,
n
=
p
×
q
n=p×q).

Explanation:

In RSA, the public key is

(
e
,
n
)
(e,n), and it's used for encryption.

The private key is
(
d
,
n
)
(d,n), and it's used for decryption, using the inverse operation:

M
=
C
d
m
o
d

n
M=C
d
modn
upvoted 1 times

Question #15 *Topic 1*

Terrance is trying to describe steganography to a new employee in the security department. For this first discussion, Terrance just wants the new employee to understand the basics. The most common way steganography is accomplished is via which one of the following?

A. MSB

B. ASB

C. LSB

D. RSB

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

Denis is looking at an older system that uses DES encryption. A colleague has told him that DES is insecure due to its short key size. What is the key length used for DES?

A. 56

B. 256

C. 64

D. 128

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

Sheryl is explaining PKI to a group of non-technical executives. She first wants to identify the specific components of PKI. Which one of the following is a component of the PKI?

A. CA

B. TGT

C. OCSP

D. TGS

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #18

Topic 1

You are studying classic ciphers. You have been examining the difference between single substitution and multi-substitution. Which one of the following is an example of a multi-alphabet cipher?

A. Atbash

B. Vigenère

C. Caesar

D. Rot13

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

Juanita is attempting to hide some text into a jpeg file. Hiding messages inside another medium is referred to as which one of the following?

A. Steganalysis

B. Cryptography

C. Cryptology

D. Steganography

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

Jane is looking for an algorithm to ensure message integrity. Which of the following would be an acceptable choice?

A. MAC

B. SHA-1

C. RC4

D. AES

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

Which one of the following wireless standards uses AES using the Counter Mode-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP)?

A. WEP

B. WPA2

C. WPA

D. WEP2

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Which one of the following terms describes two numbers that have no common factors?

A. Euler's totient

B. Fermat's number

C. Convergent

D. Coprime

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

Which one of the following uses three different keys, all of the same size?

A. AES

B. RSA

C. 3DES

D. DES

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

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

A. Rijndael

B. ECC

C. Diffie-Hellman

D. RSA

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

In steganography, ______ is the data to be covertly communicated (in other words, it is the message you wish to hide.)

A. Carrier

B. Channel

C. Payload

D. Signal

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

When learning algorithms, such as RSA, it is important to understand the mathematics being used. In RSA, the number of positive integers less than or equal to some number is critical in key generation. The number of positive integers less than or equal to n that are coprime to n is called ______.

A. Fermat's number

B. Fermat's prime

C. Mersenne's number

D. Euler's totient

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!