Dashboard › My courses › In18-S8-EN4720 (117531) › General › Quiz 1

Started on	Friday, 7 April 2023, 1:55 PM
State	Finished
Completed on	Friday, 7 April 2023, 2:15 PM
Time taken	20 mins 1 sec
Marks	17.00/20.00
Grade	**8.50** out of 10.00 (**85**%)

Question 1

Correct

Mark 1.00 out of 1.00

When the plaintext “SUN” is encrypted with Ceaser’s cipher with the key being two (2,) the ciphertext is,

○ a. WUP

○ b. QSL

● c. UWP ✓

○ d. NUS

Your answer is correct.

The correct answer is:
UWP

Question 2

Correct

Mark 1.00 out of 1.00

AES has three different configurations based on the number of rounds and key size.

○ a. False

● b. True ✓

Your answer is correct.

The correct answer is:
True

Question 3

Correct

Mark 1.00 out of 1.00

If you have a strong authentication and authorization mechanism, it can provide non-repudiation as well, assuming that social engineering attacks are not possible.

● a. True ✓

○ b. False

Your answer is correct.

The correct answer is:
True

Question **4**

Correct

Mark 1.00 out of 1.00

Block ciphers accumulate symbols in a message of a ______

○ a. Variable

● b. Fixed size ✓

○ c. All of these answers are correct

○ d. Integration

Your answer is correct.

The correct answer is:
Fixed size

Question **5**

Correct

Mark 1.00 out of 1.00

In the context of Public Key Infrastructure (PKI), which entity is responsible for issuing digital certificates and managing their lifecycle?

● a. Certificate Authority (CA) ✓

○ b. End User

○ c. Registration Authority (RA)

○ d. Certificate Subject

Your answer is correct.

The correct answer is:
Certificate Authority (CA)

Question 6

Correct

Mark 1.00 out of 1.00

Which one of the following statements is false about RSA?

○ a. RSA OAEP adds randomness to the plaintext.

● b. Textbook RSA is semantically secure ✓

○ c. Textbook RSA is vulnerable to plaintext guessing attacks.

○ d. None of these statements are false about RSA

Your answer is correct.

The correct answer is:
Textbook RSA is semantically secure

Question 7

Correct

Mark 1.00 out of 1.00

Which of the following attacks on digital certificates aims to find a hash collision in order to forge a certificate with a valid signature?

○ a. Replay attack

● b. Birthday attack ✓

○ c. Man-in-the-middle attack

○ d. Brute force attack

Your answer is correct.

The correct answer is:
Birthday attack

Question 8

Correct

Mark 1.00 out of 1.00

Hash function are used in which one of the following?

○ a. Message authentication codes

○ b. RSA OAEP

● c. All of these answers are correct ✓

○ d. Digital signatures

Your answer is correct.

The correct answer is:
All of these answers are correct

Question 9

Incorrect

Mark 0.00 out of 1.00

Alice and Bob are exchanging keys using the DH Protocol. Can Alice guarantee that she is communicating with Bob?

○ a. Yes, by adding an extra step for authentication

○ b. None of these answers are correct

○ c. Yes, by sharing a password known by both parties in an encrypted message

● d. No, it is impossible, as DH protocol is not secure against active attacks ✖

Your answer is incorrect.

The correct answer is:
Yes, by adding an extra step for authentication

Question **10**

Correct

Mark 1.00 out of 1.00

What makes MAC different from a hash function?

○ a. Hash function

○ b. Message

● c. Secret key ✓

○ d. Encryption algorithm

Your answer is correct.

The correct answer is:
Secret key

Question 11

Correct

Mark 1.00 out of 1.00

Which one of the following algorithms are not used in asymmetric-key cryptography?

○ a. Blowfish

○ b. RSA algorithm

○ c. DSA algorithm

● d. Diffie-Hellman algorithm ✗

Your answer is correct.

The correct answer is:
Blowfish

Comment:

Question **12**

Correct

Mark 1.00 out of 1.00

OAEP enhanced RSA security based on which main concept?

● a. One-wayness ✖

○ b. All or nothing

○ c. Hardness of factoring

○ d. Collision resistance

Your answer is correct.

The correct answer is:
All or nothing

Comment:

Question 13

Incorrect

Mark 0.00 out of 1.00

Consider the message space M ∊ {0,1}^2 and key space K ∊ {00,01}. A message (m) is encrypted using the one-time pad with a key (k) to produce a ciphertext (c). What is the incorrect statement?

● a. Pr[C=c|M=m] = Pr[C=c] ✓

○ b. If c=11, the message can only be 10 or 11

○ c. Pr[M=m] = ¼

○ d. Pr[M=m|C=c] = ½

Your answer is incorrect.

The correct answer is:
Pr[C=c|M=m] = Pr[C=c]

Comment:

Question 14

Correct

Mark 1.00 out of 1.00

Consider a situation where an adversary knows the length of a password, and upon observing the ciphertext, he/she derives that some digits are repetitively used in the password. In this scenario, is the posterior distribution of the plaintext the same as the prior distribution?

○ a. Yes

○ b. No

Your answer is correct.

The correct answer is:
No

Comment:

Question **15**

Correct

Mark 1.00 out of 1.00

An initialization vector (IV) or starting variable (SV) is a block of bits that is used by several modes to _____.

○ a. Randomize the encryption

○ b. None of these answers are correct

○ c. Minimize and Maximize the randomization

○ d. Randomize the decryption

Your answer is correct.

The correct answer is:
Randomize the encryption

Comment:

Question 16

Correct

Mark 1.00 out of 1.00

If Alice wants to sign a message to Bob, Alice should encrypt with;

○ a. Alice's Public Key

○ b. Alice's Private Key

○ c. Bob's Public Key

○ d. Bob's Private Key

Your answer is correct.

The correct answer is:
Alice's Private Key

Comment:

Question 17

Correct

Mark 1.00 out of 1.00

With symmetric key algorithms, the ____ key is used for the encryption and decryption of data.

○ a. None of these answers are correct

○ b. Either different keys or the same key, depending on the setup

○ c. Different

○ d. Same

Your answer is correct.

The correct answer is:
Same

Comment:

Question 18

Correct

Mark 1.00 out of 1.00

Which of the following statements is false?

○ a. Symmetric key encryption is typically more secure than public key infrastructures.

○ b. None of these answers are correct

○ c. In the public key setup, N (according to the notation used in class) is a uniformly random number

○ d. Symmetric key encryption is typically faster than public key encryption.

Your answer is correct.

The correct answers are:
Symmetric key encryption is typically more secure than public key infrastructures.,

In the public key setup, N (according to the notation used in class) is a uniformly random number

Comment:

Question 19

Incorrect

Mark 0.00 out of 1.00

Which of the following can be considered hash functions?

○ a. MD5

○ b. BLAKE

○ c. Whirlpool

○ d. All of these answers are correct

Your answer is incorrect.

The correct answer is:
All of these answers are correct

Comment:

Question 20

Correct

Mark 1.00 out of 1.00

Which of the following is/are offered by the Hash functions depending on their usage in different scenarios together with other cryptographic primitives?

○ a. Authentication

○ b. Non-repudiation

○ c. All of these answers are correct

○ d. Data integrity

Your answer is correct.

The correct answer is:
All of these answers are correct

Comment:

Previous activity

◄ Overleaf file for exercises, assignments and extra readings

Jump to...

Next activity

Programming Assignment ►

Stay in touch

University of Moratuwa

https://uom.lk

0094 11 26 400 51

info[AT]uom[.]lk

f in

Data retention summary

Get the mobile app