Started on	Friday, 12 November 2021, 5:30 PM
State	Finished
Completed on	Friday, 12 November 2021, 6:04 PM
Time taken	33 mins 59 secs
Grade	**8.00** out of 10.00 (**80**%)

Question 1

Incorrect

Mark 0.00 out of 1.00

Flag question

Suppose your friend has proposed a Message Authentication Code (MAC) algorithm. The message "m" is first divided into 16-nibble pieces (with zeroes padded to the end of the message to obtain a multiple of 16). Then all of the pieces are XORed together to obtain a 16-nibble result. To generate the t-nibble length tag, the MAC function is then applied to the shorter result.

Now it is your turn to check the security of this scheme. Your computer supports the binary representation of a character (in standard character set) to fit into 1 byte. Suppose you have two inputs and ignore the 'space':

1. Yes I have your code and input and logic
2. Yes I have your code and logic and input

Now consider the following statements:

(a) The algorithm works properly for these inputs.
(b) The algorithm does not work properly for these inputs.
(c) No security in this MAC algorithm.
(d) MAC algorithm is secure.

Determine the following which is true?

Select one:

○ b and c are true

○ a and d are true

○ b and d are true

● a and c are true ✗

Your answer is incorrect.

The correct answer is: b and c are true

Question 2

Correct

B receives the message M = (1101, 011), supposedly sent by his friend. The right part of the received message is an enciphered hash of the left part, using the following matrix

A = | 1 0 1 1 |

Mark 1.00 out of 1.00

Flag question

| 0 1 0 0 |

| 1 1 0 1 |

The secret key K = 001 used to encipher the hash is a Vernam cipher Key known only to B and his friend.

Select one:

● B should be doubtful about the source of the communication ✓

○ B should accept the message as a valid communication

Your answer is correct.

The correct answer is: B should be doubtful about the source of the communication

Question 3

Correct

Mark 1.00 out of 1.00

Flag question

Let A be a binary matrix with k rows and n columns. Let M be a message with the form of a binary string of length n. Construct a simple hash function such that the hash of M has length k.

If A= | 1 0 1 1 |

| 0 1 0 0 |

| 1 1 0 1 |

and K = 1101

The hash of M is

Select one:

○ 111

● 011 ✓

○ 110

○ 101

Your answer is correct.

The correct answer is: 011

Question 4

Incorrect

Mark 0.00 out of 1.00

Flag question

Suppose that Bob sends an authenticated message to Alice. Now consider the following scenario:

1. Alice may forge a different message and claim that it came from John.

2. John can deny sending the message.

Determine the following which is true?

Select one:

● 1 is false ✗

○ Both are true

○ Both A and B are false

○ 2 is false

Your answer is incorrect.

The correct answer is: Both are true

Question **5**

Correct

Mark 1.00 out of 1.00

Flag question

Keccak, the NIST standard SHA3 Hash is based on the

Select one:

○ AES

● Permutation ✓

○ 3-DES

○ RSA

Your answer is correct.

The correct answer is: Permutation

Question **6**

Correct

Mark 1.00 out of 1.00

Flag question

The generators associated with prime 7 are

Select one:

○ 3, 6

○ 3, 4

● 3, 5 ✓

○ 3, 2

Your answer is correct.

The correct answer is: 3, 5

Question **7**

Correct

Mark 1.00 out of 1.00

Flag question

A cryptographic software uses a key length of 160 bits. These 160 bits are derived as follows: the software repeatedly selects 20 random characters from the set {a, …, z} and that here 8 bits are used to encode each character. Therefore, the key length is 8 ∗ 20 = 160 bits long. Determine the number of operations required to attack the cipher with respect to brute force attack.

Select one:

○ 2^{26}

○ 2^{160}

● 26^{20} ✓

○ 26^{160}

Your answer is correct.

The correct answer is: 26^{20}

Question 8

Correct

Mark 1.00 out of 1.00

Flag question

Suppose you have to implement a hash function, ‘h’ with the following properties:

(i) Given a message m, the message digest h(m) can be calculated very quickly

(ii) h is a one-way, or preimage resistant function

(iii) The function h is said to be strongly collision-free

Now you have designed the function as follows:

h(m) = m (mod n), where n is a positive integer.

Now determine the following:

Select one:

○ The function neither satisfy (i), nor (ii), nor (iii)

○ The function satisfies (i) and (ii), but not (iii)

● The function satisfies (i), but not (ii) and (iii) ✓

○ The function satisfies all

Your answer is correct.

The correct answer is: The function satisfies (i), but not (ii) and (iii)

Question 9

Correct

Mark 1.00 out of 1.00

Flag question

For an easy version of Discrete-log problem, the value of x is as follows, when p = 11 and remainder(2^x) = 9

Select one:

○ 5

○ 10

○ 9

● 6 ✓

Your answer is correct.

The correct answer is: 6

Question 10

Correct

Mark 1.00 out of 1.00

A and B try to agree on a common secret key K by Diffie-Hellman key exchange. Here, p (=11) is a prime that is publicly chosen, and g (=2) is a generator for p. If a (=4) and b (=3) are the secret numbers chosen by A and B respectively then the common secret key K agreed between A and B is

Flag question

Select one:

● 4 ✓

○ 3

○ 8

○ 9

Your answer is correct.

The correct answer is: 4

Finish review

QUIZ NAVIGATION

1 2 3 4 5 6 7 8 9 10

Show one page at a time

Finish review

You are logged in as Siba Smarak Panigrahi *Log out*