Old MM Quiz 3

Due Oct 25 at 9am **Points** 10 **Questions** 7
Available until Oct 25 at 9am **Time Limit** None
Allowed Attempts Unlimited

Instructions

This is a mid-module quiz from a previous semester.

It is not necessarily representative of what this semester's quiz will look like, but is good practice.

It is worth a small amount toward your grade.

It will close 24 hours before this semester's quiz.

You may take it as many times as you wish.

You may work on it alone or collaborate with others.

You may use course materials and your own notes and homework during the quiz.

Do not give away answers to people you are not collaborating with.

This quiz was locked Oct 25 at 9am.

Attempt History

	Attempt	Time	Score
KEPT	Attempt 2	2 minutes	10 out of 10
LATEST	Attempt 2	2 minutes	10 out of 10
	Attempt 1	1,485 minutes	9 out of 10

Correct answers are hidden.

Score for this attempt: **10** out of 10
Submitted Oct 24 at 6:30pm
This attempt took 2 minutes.

Question 1

1 / 1 pts

We learned in class about "divisionless mod" where x mod y is computed in steps. One step is to consider y in the form of 2^a - b. When y is 250, what are a and b?

a = 8

b = 6

Answer 1:

8

Answer 2:

6

Question 2

1 / 1 pts

We learned in class about "divisionless mod" where x mod y is computed in steps. One step is to break x into two pieces. If a=6, b=1 and x=F11 (in hex), what are xhi and xlo? Write your answers in binary with no spaces or leading zeros.

xhi = 111100

xlo = 010001

Answer 1:

111100

Answer 2:

010001

Question 3

1 / 1 pts

We learned in class about "divisionless mod" where x mod y is computed in steps. One step is to use xhi, xlo, a and b to compute a value that is congruent to x mod y. If xhi=14, xlo=4, a=5, and b=3, what is the computed value?

46

Question 4

1 / 1 pts

For each dropdown, select the answer that best matches the definition of the cryptographic hash property for H.

Pre-image resistance: Given b , it is hard to find a such that [Select] .

Second pre-image resistance: Given [Select] , it is hard to find [Select] such that [Select] .

Collision resistance: Given [Select] , it is hard to find [Select] such that H(a)=H(b) .

Answer 1:

b

Answer 2:

a

Answer 3:

H(a)=b

Answer 4:

b

Answer 5:

a!=b

Answer 6:

H(a)=H(b)

Answer 7:

nothing

Answer 8:

a!=b

Answer 9:

H(a)=H(b)

Question 5

1 / 1 pts

If a correct algorithm is written with the following structure:

```
ASolver(x):
   ...
   BSolver(x')
   ...
   return x solution
```

Which of the following logical implications does the algorithm establish? Select all that apply.

☐ ASolver exists implies BSolver exists

☑ BSolver exists implies ASolver exists

☑ ASolver doesn't exist implies BSolver doesn't exist

☐ BSolver doesn't exist implies ASolver doesn't exist

Question 6

2 / 2 pts

Consider the following version of Horner's method which computes a polynomial hash of (a_1, a_2, ..., a_n) using randomly chosen k (all values in Z_p.)

```
   acc = k
   for i = 1 to n
      acc = (acc + a[ i ]) % p
      acc = (acc * k) % p
   return acc
```

It is ε-almost-universal for which ε? Choose the

○ n/p

● (n+1)/p

○ n/(p+1)

○ (n+1)/(p+1)

Question 7

3 / 3 pts

Consider the following collection of hash functions $Z_5 \rightarrow Z_4$.

```
          hash functions
        h1  h2  h3  h4  h5  h6
I  0 |   0   2   2   3   0   1
n  1 |   2   3   0   1   0   2
p  2 |   1   0   2   3   2   0
u  3 |   1   3   0   2   0   1
t  4 |   3   2   1   1   2   0
s
```

Each column h1 - h6 represents a function's outputs for the inputs listed on the left.

What pair of inputs maximizes the probability of collision? Write your answer as a pair of integers separated by a comma without any spaces (for example "6,8"). 1,3

For what ε is this collection of hash functions ε-almost-universal? Write your answer as a pair of integers separated by a slash without any spaces (for example "6/8") 3/6

Answer 1:

1,3

Answer 2:

3/6

Quiz Score: **10** out of 10