MM Quiz 3

Started: Oct 26 at 6:48pm

Quiz Instructions

This is your mid-module quiz. Unlike the old quiz you did for homework, it is not collaborative. Once you start the quiz you will have a limited amount of time to complete it.

Be careful with formatting. If I specify a formatting method and you do not follow it, you will lose some credit.

The quiz is open notes. You may use your own notes and any of the resources on the course webpages. You are not allowed to use the internet for any other purpose unless a question directs you to do so.

On the day of the quiz, do not use any public forum to ask any quiz-related questions. Once you see the quiz, do not discuss it with anyone until the quiz closes for everyone.

Good luck!

Question 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 120, what are a and b?

a = 7

b = 8

Question 2 — 1 pts

We learned in class about "divisionless mod" where x mod y is computed in steps. One step is to break x into to pieces. If a=8, b=3 and x=F11 (in hex), what are xhi and xlo? Write your answers in binary with no spaces or leading zeros.

xhi = 1111

xlo = 00010001

Question 3 — 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=7, xlo=6, a=5, and b=3, what is the computed value?

27

Question 4 — 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 [H(a)=b] .

Second pre-image resistance: Given [b] , it is hard to find [a!=b] such that [H(a)=H(b)] .

Collision resistance: Given [nothing] , it is hard to find [a!=b] such that [H(a)=H(b)] .

Question 5

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
- [x] BSolver exists implies ASolver exists
- [x] ASolver doesn't exist implies BSolver doesn't exist

- [ ] BSolver doesn't exist implies ASolver doesn't exist

Question 6 — 3 pts

Consider the following version of Horner's method which computes a polynomial with coefficients a_1, a_2, ..., a_n and variable k. You may want to write out the polynomial it computes.

```
acc = k
for i = 1 to n
   acc += a[ i ]
   acc *= k
return acc
```

What is the degree (ie, k's exponent) of the highest-degree term?

n

What is the coefficient of the highest-degree term? a[1]

What is the degree (ie, k's exponent) of the lowest-degree term?

0

What is the coefficient of the lowest-degree term? a[n]

Question 7 — 2 pts

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

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

No new data to save. Last checked at 7:30pm

Submit Quiz