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?

y = 250

x mod y

x mod 250

$256 - 6$

$2^8 - 6$

$2^a - b$

a = 8

b = 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

x mod y

3,857 mod y

$2^a - b$

$= 2^6 - 1$

$= 63$

x = 1111 0001 0001

lo

hi

$x_{hi} = 111100$

$x_{lo} = 010001$

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?

Given: $x_{hi} = 14$ $a = 5$

$x_{lo} = 4$ $b = 3$

$x = x_{hi} * b + x_{lo}$

$= 14 * 3 + 4$

$= 46$

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] H(a) = b .

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

Collision resistance: Given [Select] nothing , it is hard to find [Select] a != b such that 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
- [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

From lecture notes

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)

$$Poly_k(M) = a_1 P + a_2 P + \ldots + a_M k$$

$$\therefore \frac{(n+1)}{P}$$

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

(0, 1) 1/6

(0, 2) 2/6 (1, 2) 0

(0, 3) 2/6 (1, 3) 3/6 (2, 3) 1/6

(0, 4) 1/6 (1, 4) 1/6 (2, 4) 2/6 (3, 4) 0