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 120, what are a and b?

a = 7

b = 8

$2^a - b$

x mod y

↑

120

↑

$2^7 - 8$

a = 7

b = 8

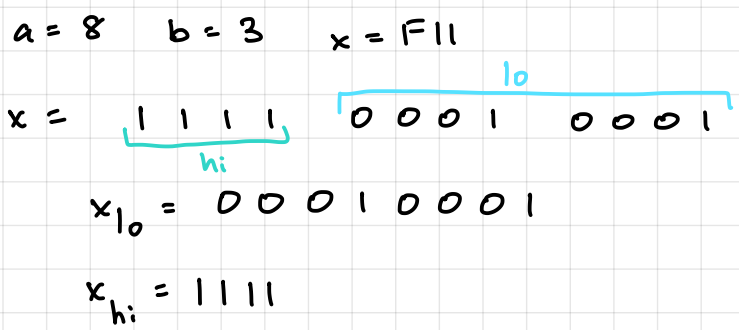
Question 2

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 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 / 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

$x_{hi} = 7 \quad x_{lo} = 6 \quad a = 5 \quad b = 3$

$$x = x_{hi} * b + x_{lo}$$
$$= 7 * 3 + 6$$
$$= 21 + 6$$
$$= 27$$

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

Question 6

0.75 / 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?

What is the coefficient of the highest-degree term?

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

What is the coefficient of the lowest-degree term?

$acc = k + a[1]$

$acc = (k + a[1])k = k^2 + a[1]k$

$acc = (k^2 + a[1]k) + a[2]$

$acc = (k^2 + a[1]k + a[2])k$

$= k^3 + a[1]k^2 + a[2]k$

$acc = (k^3 + a[1]k^2 + a[2]k) + a[3]$

$acc = (k^3 + a[1]k^2 + a[2]k + a[3])k$

$= k^4 + a[1]k^3 + a[2]k^2 + a[3]k$

a) Degree of highest degree term: n

b) Coefficient of highest degree: 1

c) Degree of lowest degree term: 1

D) Coefficient of lowest degree: $a[n]$

Question 7

2 / 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

$(0,1) = 1/6$

$(0,2) = 1/6$ $\quad (1,2) = 0$

$(0,3) = 1/6$ $\quad (1,3) = 3/6$ $\quad (2,3) = 0$

$(0,4) = 1/6$ $\quad (1,4) = 2/6$ $\quad (2,4) = 1/6$ $\quad (3,4) = 1/6$