## 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
Question i	ı pa

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?

Question 2 1 pts

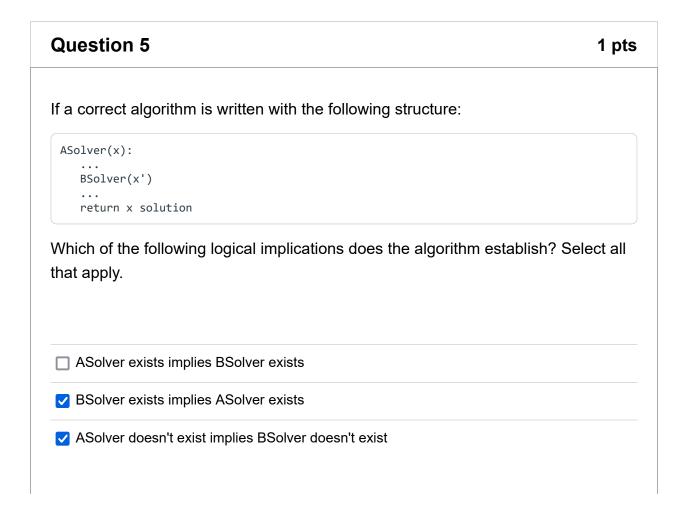
We learned in class about "divisionless mod" where x mod y is computed in steps. One step is to break x into to pieces. If a=8, b=3 and x=F11 (in hex), what are xhi and xlo? Write your answers in binary with no spaces or leading zeros.

xhi =	1111
xlo =	00010001

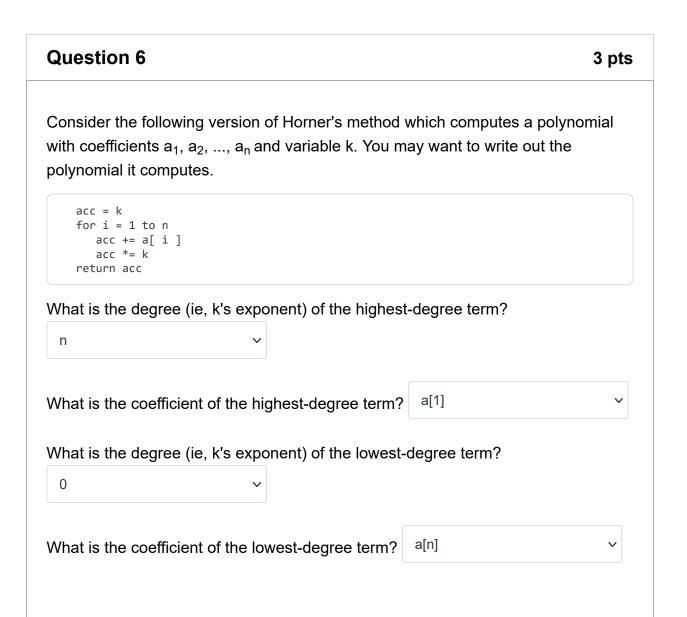
Question 3	1 pts
We learned in class about "divisionless mod" where x mod y is computed in One step is to use xhi, xlo, a and b to compute a value that is congruent to y. If xhi=7, xlo=6, a=5, and b=3, what is the computed value?	•
27	

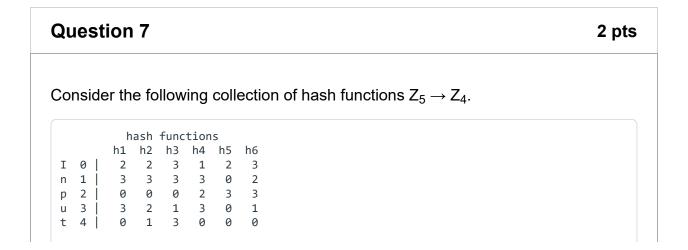
Question 4	1 pts

Pre-image resistance: Given	b	<b>v</b>	, it is hard to find
а		H(a)=b	<b>~</b> .
Second pre-image resistance	e: Given b		, it is hard to
find a!=b	∨ such t	that H(a)=H(b)	<b>v</b> .
find a!=b  Collision resistance: Given	such t		it is hard to find



■ BSolver doesn't exist implies ASolver doesn't exist





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  $\epsilon$  is this collection of hash functions  $\epsilon$ -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