Old EOM Quiz 3

Due Nov 3 at 9am **Points** 20 **Questions** 5
Available until Nov 3 at 9am **Time Limit** None
Allowed Attempts Unlimited

Instructions

This is an end-of-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.

Take the Quiz Again

Attempt History

	Attempt	Time	Score
KEPT	Attempt 8	less than 1 minute	16 out of 20 *
LATEST	Attempt 8	less than 1 minute	16 out of 20 *
	Attempt 7	less than 1 minute	14 out of 20 *
	Attempt 6	10 minutes	10 out of 20 *
	Attempt 5	less than 1 minute	6 out of 20 *
	Attempt 4	1 minute	6 out of 20 *
	Attempt 3	12 minutes	6 out of 20 *
	Attempt 2	less than 1 minute	6 out of 20 *

Attempt	Time	Score
Attempt 1	409 minutes	6 out of 20 *

* Some questions not yet graded

ⓘ Correct answers are hidden.

Score for this attempt: **16** out of 20 *
Submitted Nov 2 at 12:18pm
This attempt took less than 1 minute.

Question 1

4 / 4 pts

Select each correct statement.

- [x] If a cryptographic hash function is collision resistant, then it is preimage resistant.
- [ ] If a cryptographic hash function is preimage resistant, then it is collision resistant.
- [ ] HMAC uses almost-universal hashing to produce an authentication tag.
- [ ] Wegman-Carter authentication uses a cryptographic hash to produce an authentication tag.
- [ ] Fast cryptographic hashes are faster than fast almost-universal hashes.

Question 2

4 / 4 pts

Recall that divisionless modular reduction computes the mod of 2^a-b without using division. What mod is being performed by the following code snippet? Give your answer by telling me the a and b of the modulus.

```
x = (x >> 8) + (x & 0xFF);
```

a = 8

b = 1

Answer 1:

8

Answer 2:

1

Question 3

4 / 4 pts

Consider the following version of Horner's method which computes a polynomial with coefficients a_1, a_2, ..., a_n and variable k.

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

Determine precisely what polynomial is being computed and answer the following questions about it.

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

What is the coefficient of the highest-degree term? 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]

Answer 1:

n

Answer 2:

1

Answer 3:

0

Answer 4:

a[n]

Question 4

4 / 4 pts

This problem will test your understanding of the sponge construction by having you simulate it. The internal function used will be the permutation p : $\{0,1\}^8 \rightarrow \{0,1\}^8$ where p(x) = x <<< 1 (an 8-bit permutation where x is rotated left one bit). We will use rate R = 4 bits and capacity C = 4 bits.

Let's say that after padding your data is 10101001. After the second invocation of p (ie, after absorbing this data), what is the value of your chaining block?

Give your answer as a sequence of bits without spaces or other characters (ie, use the characters 0 and 1 for your answers and nothing else).

10100011

Unanswered

Question 5

Not yet graded / 4 pts

Ignore this question. It is a placeholder for your programming quiz score.

Do the programming problem at

https://class.mimir.io/assignments/2949d98a-4c6a-4514-9197-f837dc6255e9 (https://class.mimir.io/assignments/2949d98a-4c6a-4514-9197-f837dc6255e9)

before it closes and those points will be copied here later.

Your Answer:

Quiz Score: **16** out of 20