MM Quiz 5

Due Dec 2 at 10pm   **Points** 10   **Questions** 4
Available Dec 2 at 9am - Dec 2 at 10pm about 13 hours   **Time Limit** 50 Minutes

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!

This quiz was locked Dec 2 at 10pm.

Attempt History

	Attempt	Time	Score
LATEST	[Attempt 1](#)	49 minutes	7.5 out of 10

⚠ Correct answers are hidden.

Score for this quiz: **7.5** out of 10
Submitted Dec 2 at 8:03pm
This attempt took 49 minutes.

Question 1	2.5 / 2.5 pts

A trick die has eight sides that are equally likely to face up. The

numbers on the eight sides are 1, 2, 3, 4, 1, 6, 7, 8. That's right, two sides are marked 1 and none are marked 5. How many bits of entropy are there with respect to what number faces up when the die is rolled? Round your answer to the nearest hundredth.

2.75

Incorrect

Question 2   0 / 2.5 pts

Each of the following is a true/false statement about a tweakable block cipher (TBC). Place a checkmark next to each true statement.

In the questions mentioning E', let E' be a random instance of a TBC and E'(T,X) be the result of using E' with tweak T and input X.

F ☐
For TBC security both the current key and tweak in use must be kept secret from adversaries.

T ☐
Each time a new tweak is given to a TBC, the TBC behaves like a new random permutation.

T ☑
When a TBC is used once per tweak its outputs may be considered uniformly distributed.

T ☐ A TBC is a prominent part of the design of OCB.

T ☐ If X1 ≠ X2, then always E'(T,X1) ≠ E'(T,X2)

F ☑ If T1 ≠ T2, then always E'(T1,X) ≠ E'(T2,X)

Question 3

2.5 / 2.5 pts

I showed you in lecture how OCB uses a tweakable block cipher (TBC). It uses the universal hash function $h(T) = (iv)2^T$ where each message has its own random iv and calculation is over a Galois field. The TBC is then constructed as $E'(T,X) = h(T)$ xor $E(X$ xor $h(T))$. This hash function is optimized for finding $h(T+1)$ given $h(T)$.

For this problem we'll use $GF(2^8)$ whose modulus is $x^8 + x^4 + x^3 + x + 1$. If $h(0)$ is 11001101 (in binary or CD in hex), what are $h(1)$ and $h(2)$?

h(1) 81

h(2) 19

Answer each with exactly 8 binary digits or 2 hex digits, and no spaces.

Answer 1:

81

Answer 2:

19

Question 4

2.5 / 2.5 pts

Let's now say that we are using as our block cipher the S-box from AES (ie, imagine that we have given a block cipher a key and it has given us the AES S-box as our permutation to use).

If $h(0)$ = 11001101 (in binary or CD in hex), then using the construction and hash function from the previous problem, what are the following values?

E'(1, 00000000) 8D

E'(2, 10101010)   74

Answer each with exactly 8 binary digits or 2 hex digits, and no spaces. You can find the AES S-box on Page 101 of https://www.crypto-textbook.com/download/Understanding-Cryptography-Chapter4.pdf   [(https://www.crypto-textbook.com/download/Understanding-Cryptography-Chapter4.pdf)](https://www.crypto-textbook.com/download/Understanding-Cryptography-Chapter4.pdf)

Answer 1:

   8D

Answer 2:

   74

Quiz Score: **7.5** out of 10