MM Quiz 2

Due Oct 5 at 10pm **Points** 10 **Questions** 3
Available Oct 5 at 9am - Oct 5 at 10pm about 13 hours **Time Limit** 40 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 Oct 5 at 10pm.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	40 minutes	8.75 out of 10

ⓘ Correct answers are hidden.

Score for this quiz: **8.75** out of 10
Submitted Oct 5 at 6:04pm
This attempt took 40 minutes.

Question 1 — 5.5 / 5.5 pts

You are to *decrypt* a ciphertext that was *encrypted* using the

permutation p : $\{0,1\}^4 \rightarrow \{0,1\}^4$ defined as p(x) = ~(x >>> 1), ie, rotate x RIGHT 1 bit and then negate all the bits. For example p(0011) = 0110 because 0011>>>1 = 1001 and ~1001 = 0110. Thus $p^{-1}(x)$ = (~x <<< 1). If you need an IV use 0101. If you need a nonce use 01. If the mode uses padding to handle arbitrary plaintext lengths, remove 10* padding. If you need a counter, begin at 1.

Decrypt the ciphertext 1110 0001 1010 given that it was produced using ECB mode. Write four bits per box, with the final box possibly having fewer bits.

0010	1101	10

Decrypt the ciphertext 1110 0001 1010 given that it was produced using CBC mode. Write four bits per box, with the final box possibly having fewer bits.

0111	0011	101

Decrypt the ciphertext 1110 0001 1010 given that it was produced using CTR mode. Write four bits per box, with the final box possibly having fewer bits.

1011	1101	1110

Decrypt the ciphertext 1110 0001 1010 given that it was produced using OFB mode. Write four bits per box, with the final box possibly having fewer bits.

1011	0100	1111

Answer 1:

0010

Answer 2:

1101

Answer 3:

10

Answer 4:

0111

Answer 5:

0011

Answer 6:

101

Answer 7:

1011

Answer 8:

1101

Answer 9:

1110

Answer 10:

1011

Answer 11:

0100

Answer 12:

1111

Partial

Question 2

2.25 / 3 pts

GF(8) is defined like GF(256) except the polynomials all have degree less than 3 and the modulus is $x^3 + x + 1$. Calculate the following. Give

each of your answers as exactly three binary digits.

011 × 010 = 110

100 × 010 = 010 <-- Correct Answer: 011

110 × 100 = 101

011 + 010 = 001

Answer 1:

110

Answer 2:

010

Answer 3:

101

Answer 4:

001

Question 3

1 / 1.5 pts

Let's say you are designing a secure communication system that has two AES units in it (ie, it can compute AES or AES^{-1} on two blocks at the same time). Also, let's say that security, encryption speed, and decryption speed are all equally important to you. Which mode-of-operation would you select? Explain your answer in one or two sentences.

Your Answer:

I would choose either ECB or CTR since encryption and decryption can be done in parallel in these two modes.

CTR is the only secure mode of the four we studied that allows parallel encrypt and decrypt.

NOTE: ECB allows parallel encrypt and decrypt, but is unsecure compared to CTR

Quiz Score: **8.75** out of 10