Old MM Quiz 2

Due Oct 4 at 9am **Points** 10 **Questions** 3
Available until Oct 4 at 9am **Time Limit** None
Allowed Attempts Unlimited

Instructions

This is a mid-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 3	2 minutes	10 out of 10
LATEST	Attempt 3	2 minutes	10 out of 10
	Attempt 2	4 minutes	9.58 out of 10
	Attempt 1	166 minutes	9.17 out of 10

ⓘ Correct answers are hidden.

Score for this attempt: **10** out of 10
Submitted Oct 1 at 1:02am

This attempt took 2 minutes.

Question 1

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. Thus $p^{-1}(x) = (x <<< 1)$. If you need an IV use 1001. If you need a nonce use 10. If the mode uses padding to handle arbitrary plaintext lengths, remove 10* padding. If you need a counter, begin at 1.

Decrypt the ciphertext 0011 0101 0110 given that it was produced using ECB mode. Write four bits per box, with the final box possibly having fewer bits.

0110	1010	1

Decrypt the ciphertext 0011 0101 0110 given that it was produced using CBC mode. Write four bits per box, with the final box possibly having fewer bits.

1111	1001	100

Decrypt the ciphertext 0011 0101 0110 given that it was produced using CTR mode. Write four bits per box, with the final box possibly having fewer bits.

1111	0000	1011

Decrypt the ciphertext 0011 0101 0110 given that it was produced using OFB mode. Write four bits per box, with the final box possibly having fewer bits.

1111	0011	0101

Answer 1:

0110

Answer 2:

1010

Answer 3:

1

Answer 4:

1111

Answer 5:

1001

Answer 6:

100

Answer 7:

1111

Answer 8:

0000

Answer 9:

1011

Answer 10:

1111

Answer 11:

0011

Answer 12:

0101

Question 2

3 / 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.

010 × 010 = 100

011 × 011 = 101

101 × 101 = 111

010 + 010 = 000

Answer 1:

100

Answer 2:

101

Answer 3:

111

Answer 4:

000

Question 3

2 / 2 pts

Let's say that you receive a ciphertext that was encrypted with a b-bit permutation and is nb-bits in length. (That is you receive an n-block ciphertext.) But, you did not receive an IV or nonce (if one was needed)

along with the ciphertext. For each of the following modes indicate how many ciphertext blocks you could correctly decrypt into plaintext blocks without knowing an IV or nonce.

ECB: n

CBC: n-1

CTR: 0

OFB: 0

Answer 1:

n

Answer 2:

n-1

Answer 3:

0

Answer 4:

0

Quiz Score: **10** out of 10