Old EOM Quiz 2

Due Oct 13 at 9am **Points** 20 **Questions** 5
Available until Oct 13 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 2	1 minute	20 out of 20
LATEST	Attempt 2	1 minute	20 out of 20
	Attempt 1	1,469 minutes	19 out of 20

Correct answers are hidden.

Score for this attempt: **20** out of 20
Submitted Oct 11 at 1:59pm
This attempt took 1 minute.

Question 1

2 / 2 pts

Which of the following AES steps supplies NO diffusion?

● Key Addition

○ Byte Substitution

○ Shift Rows

○ Mix Columns

Question 2

2 / 2 pts

GF(8) is defined like GF(256) except the polynomials all have degree less than 3 and the modulus is $x^3 + x + 1$. Which of the following is the multiplicative inverse of 010 in GF(8)?

○ 001

○ 011

○ 110

○ 100

● None of these

Question 3

8 / 8 pts

You are to *encrypt* a ciphertext using the permutation p : $\{0,1\}^4 \rightarrow \{0,1\}^4$ defined as p(x) = ~x, ie, toggle each bit (0 to 1 and 1 to 0). If you need an IV use 1010. If you need a nonce use 01. If the mode uses padding to handle arbitrary plaintext lengths, add 10* padding. If you need a counter, begin at 1.

Encrypt the ciphertext 1110 1110 111 using ECB mode. Write four bits per box, with the final box possibly having fewer bits.

0001	0001	0000

Encrypt the ciphertext 1110 1110 111 using CBC mode. Write four bits per box, with the final box possibly having fewer bits.

1011	1010	1010

Encrypt the ciphertext 1110 1110 111 using CTR mode. Write four bits per box, with the final box possibly having fewer bits.

0100	0111	011

Encrypt the ciphertext 1110 1110 111 using OFB mode. Write four bits per box, with the final box possibly having fewer bits.

1011	0100	101

Answer 1:

0001

Answer 2:

0001

Answer 3:

0000

Answer 4:

1011

Answer 5:

1010

Answer 6:

1010

Answer 7:

0100

Answer 8:

0111

Answer 9:

011

Answer 10:

1011

Answer 11:

0100

Answer 12:

101

Question 4

4 / 4 pts

Let's say that the four bytes 02 03 04 05 were supplied to the AES MixColumns operation. Of the four bytes returned, what would be the first byte? Write using exactly two hex digits (using lower-case hex for a-f). You may look at **these slides** (https://www.crypto-textbook.com/download/Understanding_Cryptography_Chptr_4---AES.pdf) or **this** chapter (https://www.crypto-textbook.com/download/Understanding-Cryptography-Chapter4.pdf) if you wish.

00

Question 5

4 / 4 pts

Let's say that an AES-128 key was 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 04. (It's a bad key because it's not random, but we'll use it in this problem anyway.) This is used as "round key 0" what are the first four bytes in "round key 1"? Write each using exactly two hex digits (using lower-case hex for a-f). You may look at **these slides (https://www.crypto-textbook.com/download/Understanding_Cryptography_Chptr_4---AES.pdf)** or **this chapter (https://www.crypto-textbook.com/download/Understanding-Cryptography-Chapter4.pdf)** if you wish.

62	63	f2
62		

Answer 1:

62

Answer 2:

63

Answer 3:

f2

Answer 4:

62

Quiz Score: **20** out of 20