EOM Quiz 2

Due Oct 14 at 10pm **Points** 20 **Questions** 6
Available Oct 14 at 9am - Oct 14 at 10pm about 13 hours **Time Limit** 60 Minutes

Instructions

This is your end-of-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 14 at 10pm.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	60 minutes	15.5 out of 20

Correct answers are hidden.

Score for this quiz: **15.5** out of 20
Submitted Oct 14 at 4:19pm
This attempt took 60 minutes.

Partial

Question 1

1.5 / 3 pts

The security model for encryption that we learned in class involved distinguishing a black box containing real encryption from a black box that returned the same number of random bits.

For each of the following modes, if the permutation's block length is b bits, at about how many permutation calls does the mode become easy to distinguish?

Note: popup menus can't do math formatting, so sqrt is square root and pow(a,b) is a^b.

ECB 2

CTR pow(2,b)/2

Answer 1:

2

Answer 2:

pow(2,b)/2

Question 2

3 / 3 pts

These remaining problems have you simulate 1 round of AES. Each uses a different input so that if you get one step wrong it does not affect the others.

Consider the picture of AES from the **textbook reading (https://www.crypto-textbook.com/download/Understanding-Cryptography-Chapter4.pdf)** (Page 91) or **these slides (https://www.crypto-textbook.com/download/Understanding_Cryptography_Chptr_4---AES.pdf)** (Page 8). Let x and k be the following 16 bytes (in hex)

x : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
k : 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

What are the first four bytes (ie, leftmost) of the output from the first Key Addition Layer (the one at the top of the figure)? Express each byte as exactly two hexadecimal digits without any spaces.

00 01 02

03

Answer 1:

00

Answer 2:

01

Answer 3:

02

Answer 4:

03

Question 3

3 / 3 pts

These remaining problems have you simulate 1 round of AES. Each uses a different input so that if you get one step wrong it does not affect the others.

Consider the picture of AES from the **textbook reading (https://www.crypto-textbook.com/download/Understanding-Cryptography-Chapter4.pdf)** (Page 91) or **these slides (https://www.crypto-textbook.com/download/Understanding_Cryptography_Chptr_4---AES.pdf)** (Page 8). Let the input to round 1's Byte Substitution Layer be the 16 bytes

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

What are the first four bytes (ie, leftmost) of the output from round 1's Byte Substitution Layer? Express each byte as exactly two hexadecimal digits without any spaces.

63

7C

77

7B

Answer 1:

63

Answer 2:

7C

Answer 3:

77

Answer 4:

7B

Question 4

3 / 3 pts

These remaining problems have you simulate 1 round of AES. Each uses a different input so that if you get one step wrong it does not affect the others.

Consider the picture of AES from the **textbook reading (https://www.crypto-textbook.com/download/Understanding-Cryptography-Chapter4.pdf)** (Page 91) or **these slides (https://www.crypto-textbook.com/download/Understanding_Cryptography_Chptr_4---AES.pdf)** (Page 8). Let the input to round 1's Shift Rows Layer be the 16 bytes

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

What are the first four bytes of output from round 1's Shift Rows Layer? Express each byte as exactly two hexadecimal digits without any spaces.

00	05	0A
0F		

Answer 1:

00

Answer 2:

05

Answer 3:

0A

Answer 4:

0F

Partial

Question 5

1 / 4 pts

These remaining problems have you simulate 1 round of AES. Each uses a different input so that if you get one step wrong it does not affect the others.

Consider the picture of AES from the **textbook reading (https://www.crypto-textbook.com/download/Understanding-Cryptography-Chapter4.pdf)** (Page 91) or **these slides (https://www.crypto-textbook.com/download/Understanding_Cryptography_Chptr_4---AES.pdf)** (Page 8). Let the input to round 1's Mix Column Layer be the 16 bytes

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

What are the first four bytes of output from round 1's Mix Column Layer? Express each byte as exactly two hexadecimal digits without any spaces (using upper-case letters when needed).

02 03 08

07

Answer 1:

02

Answer 2:

03

Answer 3:

08

Answer 4:

07

Question 6

4 / 4 pts

These remaining problems have you simulate 1 round of AES. Each uses a different input so that if you get one step wrong it does not affect the others.

Consider the picture of AES from the **textbook reading (https://www.crypto-textbook.com/download/Understanding-Cryptography-Chapter4.pdf)** (Page 91) or **these slides (https://www.crypto-textbook.com/download/Understanding_Cryptography_Chptr_4---AES.pdf)** (Page 8). Let the input to round 1's Transform 1 be the 16 bytes

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

What are the first four bytes of output from round 1's Transform 1? Express each byte as exactly two hexadecimal digits without any spaces (using upper-case letters when needed).

D6 AA 74

FD

Answer 1:

D6

Answer 2:

AA

Answer 3:

74

Answer 4:

FD

Quiz Score: **15.5** out of 20