EOM Quiz 5

Due Dec 9 at 10pm **Points** 20 **Questions** 5
Available Dec 9 at 9am - Dec 9 at 10pm about 13 hours **Time Limit** 45 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 Dec 9 at 10pm.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	45 minutes	13.33 out of 20

Correct answers are hidden.

Score for this quiz: **13.33** out of 20
Submitted Dec 9 at 8:33pm
This attempt took 45 minutes.

Question 1

3 / 3 pts

A person grabs a shirt from a closet in the dark and puts it on. In the closet are two blue shirts, two red shirts, and four yellow shirts. How uncertain is the color of the shirt. Answer in bits of entropy, rounded to the nearest hundredth.

1.5

Incorrect

Question 2

4 / 4 pts

In the final key agreement protocol detailed in the textbook, Alice specifies a requested minimum prime p of 3 bits. What are the smallest and largest prime numbers that pass her size test?

See here for a list of primes: **https://primes.utm.edu/lists/small/10000.txt (https://primes.utm.edu/lists/small/10000.txt)**

smallest prime: 5

largest prime: 61

Answer 1:

5

Answer 2:

61

Question 3

0 / 4 pts

Consider the final key agreement protocol detailed in the textbook. If Alice and Bob are both honest, and any adversaries are passive, which of the following components could be removed and the resulting protocol would still be well-defined and secure? Check all that apply.

☑ s_a

☑ N_a

□ (p,q,g)

□ g^x

□ $Auth_B$

□ g^y

□ $Auth_A$

Question 4

5 / 5 pts

You saw a simplified version of OCB in lecture. Here's a summary. Let E'(T,X) be a tweakable block cipher that has already been keyed. Given plaintext P = P_1 || P_2 || ... || P_n (ie, P is an n-block plaintext).

C_i = E'(i, P_i) for i=1..n
sum = P_1 xor P_2 xor ... xor P_n
tag = E'(0,sum)

For simplicity let's say that E'(T,X) = ROTL(X,T+1) (ie, X rotated left T+1 bits. If the block cipher block size is 8 bits and you are encrypting the two byte plaintext 81 18 (in hex), what ciphertext and tag would be created? Fill in each box as a two-digit hex value.

C_1 06

C_2 C0

tag 33

Answer 1:

06

Answer 2:

C0

Answer 3:

33

Partial

Question 5

1.33 / 4 pts

Consider the Fortuna random generator. Choose the answer that is most correct for each statement.

Forward security is provided by Rekeying the block cipher

Consider the entropy pools P_i and P_{i+1}. In the long run, what is the ratio (number of times P_i is emptied) / (number of times P_{i+1} is emptied)?

[Select]

Consider the entropy pools P_i and P_{i+1}. In the long run, what is the ratio (number of times entropy is added to P_i) / (number of times entropy is added to P_{i+1})? [Select]

Answer 1:

Rekeying the block cipher

Answer 2:

2

Answer 3:

4

Quiz Score: **13.33** out of 20