Old EOM Quiz 5

Due Dec 8 at 9am **Points** 20 **Questions** 6
Available until Dec 8 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 20	less than 1 minute	20 out of 20
LATEST	Attempt 20	less than 1 minute	20 out of 20
	Attempt 19	less than 1 minute	17 out of 20
	Attempt 18	less than 1 minute	17 out of 20
	Attempt 17	less than 1 minute	17 out of 20
	Attempt 16	less than 1 minute	17 out of 20
	Attempt 15	less than 1 minute	17 out of 20
	Attempt 14	less than 1 minute	17 out of 20

Attempt	Time	Score
Attempt 13	less than 1 minute	17 out of 20
Attempt 12	2 minutes	17 out of 20
Attempt 11	less than 1 minute	17 out of 20
Attempt 10	less than 1 minute	17 out of 20
Attempt 9	1 minute	17 out of 20
Attempt 8	4 minutes	14.5 out of 20
Attempt 7	1 minute	14.5 out of 20
Attempt 6	2 minutes	14.5 out of 20
Attempt 5	2 minutes	14.5 out of 20
Attempt 4	5 minutes	15.75 out of 20
Attempt 3	7 minutes	11.5 out of 20
Attempt 2	28 minutes	11.5 out of 20
Attempt 1	99 minutes	9.75 out of 20

ⓘ Correct answers are hidden.

Score for this attempt: **20** out of 20
Submitted Dec 7 at 11:22am
This attempt took less than 1 minute.

Question 1

3 / 3 pts

In the final key agreement protocol detailed in the textbook, if Alice specifies her minimum acceptable prime p is 4 bits what is the smallest p she will accept from Bob.

Ignore Alice's prime test for p, just determine what's the smallest integer p that passes Alice's size test. (It goes without saying, but such a small p offers no security; I am using a small number to make the math easy.)

8

Question 2

3 / 3 pts

In the final key agreement protocol detailed in the textbook, if Alice specifies her minimum acceptable prime p is 4 bits what is the largest p she will accept from Bob.

Ignore Alice's prime test for p, just determine what's the largest integer p that passes Alice's size test. (It goes without saying, but such a small p offers no security; I am using a small number to make the math easy.)

256

Question 3

3 / 3 pts

In the final key agreement protocol detailed in the textbook, Alice specifies her minimum acceptable prime p is 4 bits. Bob must also specify a minimum number of bits for prime p. What is the smallest number of bits that Bob can require without causing Bob to abandon the exchange?

2

Question 4

3 / 3 pts

In the final key agreement protocol detailed in the textbook, let's assume that p is about 2048 bits long. Approximately how many bits of entropy are in g^{xy} mod p?

○ 2048

○ 512

● 256

○ 128

○ 0

Question 5

3 / 3 pts

In the final key agreement protocol detailed in the textbook, let's assume that p is about 2048 bits long. Approximately how many bits of entropy are in k?

○ 2048

○ 512

● 256

○ 128

○ 0

Question 6

5 / 5 pts

Which of the following are contained in a public-key infrastructure certificate? Check all that apply.

□ Owner's secret key

☑ Owner's public key

☑ Owner's name

□ A signature from the owner

□ Issuer's secret key

□ Issuer's public key

☑ Issuer's name

☑ A signature from the issuer

Quiz Score: **20** out of 20