EOM Quiz 4

Due Nov 23 at 10pm **Points** 20 **Questions** 5
Available Nov 23 at 9am - Nov 23 at 10pm about 13 hours **Time Limit** 50 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.

You may use **https://www.wolframalpha.com (https://www.wolframalpha.com/)** to help with this quiz. Some example queries that might be useful are "34^20 mod 123", "gcd(23, 25)", "123 prime?", "order of 7 mod 15", "inverse of 5 mod 13".

Good luck!

This quiz was locked Nov 23 at 10pm.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	50 minutes	16 out of 20

ⓘ Correct answers are hidden.

Score for this quiz: **16** out of 20
Submitted Nov 23 at 6:27pm
This attempt took 50 minutes.

Question 1

4 / 4 pts

Let's say that Alice and Bob are exchanging keys using Diffie-Hellman key exchange using multiplicative group Z^*_{499} and generator g=10. Let's say that Alice chooses secret exponent x=4 and receives the number 123 from Bob.

What number should Alice send to Bob? 20

What number do Alice and Bob compute as their shared secret? 331

Express each of your answers as an integer.

Answer 1:

20

Answer 2:

331

Question 2

4 / 4 pts

Consider the multiplicative group Z^*_{22}.

List all of its elements in increasing numerical order, separating each with a comma but no space. 1,3,5,7,9,13,15,17,

List all of the elements in the subgroup generated by 5 in this group, listed in increasing numerical order, separating each with a comma but no space. 1,3,5,9,15

Z^*_{22} does have at least one element that generates the entire group (ie,

a "primitive" element). Tell me one. 7

Answer 1:

1,3,5,7,9,13,15,17,19,21

Answer 2:

1,3,5,9,15

Answer 3:

7

Question 3

4 / 4 pts

Let's say that you wanted to find a subgroup of size 50 to 60 elements of the group Z*p where p is 100 to 110 following the technique seen in class.

What p would you choose? 107

What size subgroup would you find? 53

What number do you find that generates the subgroup?

4

You may find this list of primes useful: **https://primes.utm.edu/lists/small/1000.txt (https://primes.utm.edu/lists/small/1000.txt)**

Answer 1:

107

Answer 2:

53

Answer 3:

4

Question 4

4 / 4 pts

Let's say your Elgamal public key is (p, g, g^d mod p) = (13, 2, 3) and your private key is d = 4.

You receive a ciphertext (kx mod p, g^e mod p) = (6, 4).

What is the shared k value? 9

What is k^{-1} mod p? 3

What is the plaintext x? 5

Type each of your answers as an integer.

Answer 1:

9

Answer 2:

3

Answer 3:

5

Incorrect

Question 5

0 / 4 pts

Consider the elliptic-curve group defined by { (x,y) | x,y ∈ Z_{17} and x^2 mod 17 = x^3 + 2x + 2 mod 17 } (ie, the group you get when a=2, b=2, and p=17).

What is (0,11) + (5,1) in this group?

What value do you get for s? 14

What value do you get for x_3? 4

What value do you get for y_3? 1

You may find these slides useful: https://www.crypto-textbook.com/download/Understanding_Cryptography_Chptr_9---ECC.pdf (https://www.crypto-textbook.com/download/Understanding_Cryptography_Chptr_9---ECC.pdf)

Answer 1:

14

Answer 2:

4

Answer 3:

1

Quiz Score: **16** out of 20