Old EOM Quiz 4

Due Nov 24 at 9am **Points** 20 **Questions** 5
Available until Nov 24 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.

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".

Take the Quiz Again

Attempt History

	Attempt	Time	Score
KEPT	Attempt 2	5 minutes	20 out of 20
LATEST	Attempt 2	5 minutes	20 out of 20
	Attempt 1	2,809 minutes	18.67 out of 20

! Correct answers are hidden.

Score for this attempt: **20** out of 20
Submitted Nov 23 at 12:28pm
This attempt took 5 minutes.

Question 1

4 / 4 pts

Let's say you generated RSA keys and you chose p=103, q=151, and the smallest encryption exponent that qualifies for this p and q. (You will have to follow the key generation algorithm to fill in the details.)

If someone gives you 343 as the ciphertext they created using your public key, what is the plaintext you get when you use your private key to decrypt?

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".

What is the encryption exponent? 7

What is the decryption exponent? 8743

What is the resulting plaintext? 9540

Answer 1:

7

Answer 2:

8743

Answer 3:

9540

Question 2

4 / 4 pts

Consider the multiplicative group Z^*_{18}.

List all of its elements in increasing numerical order, separating each with a comma but no space. 1,5,7,11,13,17

List all of the elements generated by 7 in this group, listed in increasing numerical order, separating each with a comma but no space.

1,7,13

Z^*_{18} does have at least one element that generates the entire group (ie, a "primitive" element). Tell me one. 5

Answer 1:

1,5,7,11,13,17

Answer 2:

1,7,13

Answer 3:

5

Question 3

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=7. Let's say that Alice chooses secret exponent x=5 and receives the number 123 from Bob.

What number should Alice send to Bob? 340

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

294

Express each of your answers as an integer.

Answer 1:

340

Answer 2:

294

Question 4

4 / 4 pts

Let's say that you wanted to find a subgroup of size 10 to 15 elements of a group Z^*_p where p is 50 to 60 following the technique seen in class.

What p would you choose? 53

What size subgroup would you find? 13

What number do you find that generates the subgroup?

16

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:

53

Answer 2:

13

Answer 3:

16

Question 5

4 / 4 pts

Decrypt ciphertext (kx mod p = 7, g^e mod p = 8). The ciphertext was created using Elgamal encryption over group Z^*_p with your public key (p=13, g=2, g^d mod p=12) and your private key is d=6.

What is the shared k value? 12

What is k^{-1} mod p? 12

What is the plaintext x? 6

Type each of your answers as an integer.

Answer 1:

12

Answer 2:

12

Answer 3:

6

Quiz Score: **20** out of 20