Fall 2023 CIS 3362 Homework #6 Grading Criteria

1) 10 pts – 3 pts for what Alice sends Bob, 3 pts for what Bob sends Alice, 4 pts for their shared Key. They need to write what calculation they need to do to get the result for full credit. If they only write each of the three answers without writing down the what calculation needs to be done, just 1 pt each. (So if they only write 10, 75 and 21, just 3 pts out of 10)

2) 10 pts – 3 pts Euclidean, 5 pts Extended, 1 pt to get -661, 1 to map to 719.

3) 40 pts –

10 pts to use gcd to get common factor between two n's. If they tried to factor the two n's via one of the algorithms I provided, give max 5 pts out of 40.

5 pts to calculate phi of Alice's n
5 pts to calculate phi of Bob's n
5 pts to calculate d for Alice
5 pts to calculate d for Bob
5 pts to use d to get Alice's message to Bob.
5 pts to use d to get Bob's message to Alice.

If you feel partial is deserved, give it.

4) 40 pts –

20 pts to get Alice's private key, supporting documentation is a must with code. Long way is fine. They should report how long it took if they went that route.

20 pts to use Alice's key to decrypt the message and give partial as follows:

- 5 pts – calculate C to the a
- 5 pts – calculating K inverse mod q
- 5 pts – multiply that by C2
- 5 pts – converting number to letters