Fall 2020 CIS 3362 Homework #6 Grading Criteria (100 pts)

1) 10 pts - 4 pts for figuring out the a's are relatively prime to 42
3 pts for extracting out the values of a10, a11, a12
3 pts for stating the modular exponentiation results

2) 12 pts - 4 pts for what Alice sends to Bob
4 pts for what Bob sends to Alice
4 pts for their shared key

To get full credit, students have to show WHAT they calculated, but since I told them they could use a calculator to do the mod calculations, they don't have to do fast mod expo by hand.

3) 10 pts - 2 pts for phi(n)
7 pts extended Euclidean
1 pt to extract d and map to range

4) 12 pts - 1 pt - set up lambda
7 pts - EEA to finish solving for lambda
2 pts - solve for x
2 pts - solve for y

5) 20 pts - 10 pts for getting 2P, 10 pts for getting 4P. Breakdown for each:
6 pts total for getting lambda
2 pts for getting x
2 pts for getting y

6) 12 pts - 6 pts for each pair, 2 pts for K, 2 pts for C1, 2 pts for C2

6) 24 points

Give full credit if you decrypt and it's readable!

If it's not readable, give credit as follows:

8 pts - some function to convert a single radix 64 char to a number
8 pts - using that function to try to convert a string to a large number
8 pts - modular exponentiation

You can't give all 24 pts of course…if it doesn't work there was definitively a break down in one of these three phases, take off at least 4 pts minimum because I want to reward those who got it working.