Fall 2019 CIS 3362 Homework #5 Grading Criteria (120 pts)

Question 1: 10 pts, 2 pts per term (one for base, one for exponent)

Question 2: 12 pts, 2 pts for each term in the phi breakdown, 2 pts final answer

Question 3: 10 pts, 4 pts for stating Fermat's Thm, 4 pts for exponent breakdown, 2 pt for final solution

Question 4: 10 pts, 4 pts for stating Fermat's Thm, 4 pts for exponent breakdown, 2 pt for final solution

Question 5: 8 pts, 2 pts phi of n, 2 pts Euclidean, 3 pts Extended Euclidean, 1 pt answer in range

Question 6: 20 pts - 15 pts proof that if gcd(p-1,k) = 1 then α^k is also primitive.
5 pts for proof that if gcd(p-1,k) isn't 1, then α^k is NOT primitive
Many ways to do this proof. Give partial credit by following their logic.

Question 7: 12 pts, 2 pts for each a value, 2 pts for each primitive root

Question 8: 12 pts 3 pts for each calculation

Question 9: 26 pts - full credit if you can read the message, if you can't read the message, look to give partial credit based on the code:

3 pts - reading in text
6 pts - some sort of mechanism to convert text to a number
4 pts - some sort of mechanism to convert a single character to a number 0 to 63
5 pts - some sort of fast mod expo

These represent the maximum number of points you can award. So, for an unreadable message, the most you can award is 18 points out of 26.