

**Fall 2021 CIS 3362 Homework #6 Grading Criteria (100 pts)**

- 1) 12 pts - 4 pts for what Alice sends Bob, 4 pts for what Bob sends Alice, 4 pts for the shared key. They can use a program to simplify exponents, so just make sure that the appropriate exponents are written. If no work is shown and the answer is wrong, no pts out of 4 can be given.
- 2) 12 pts - 1 pt find phi, 3 pts Euclidean, 6 pts Extended Euclidean, 1 pt to get -33, 1 pt to map to 607.
- 3) 11 pts - 5 pts for finding lambda, 3 pts for x, 3 pts for y
- 4) 17 pts - 7 pts for finding first lambda, 2 pts for first x, 2 pts for first y, 2 pts for second lambda, 2 pts for second x, 2 pts for second y
- 5) 18 pts - 4 pts for  $Y_A$ , 1 pt for first k, 2 pts for first K, 2 pts for first C1, 2 pts for first C2  
1 pt for second k, 2 pts for second K, 2 pts for second C1, 2 pts for second C2
- 6) 30 pts - 10 pts to factor stating they used Pollard-Rho  
10 pts for using tools to get the right d.  
10 pts to decrypt