

Fall 2023 CIS 3362 Homework #6 Grading Criteria

- 1) 10 pts – 3 pts for Alice to Bob
3 pts for Bob to Alice
4 pts for shared key
Give partial as needed

- 2) 10 pts – 1 pt phi calculation (if this is wrong do 0 out of 10 total)
3 pts – Euclidean Alg
5 pts – Extended Euclidean Alg
1 pt – extracting solution correctly

- 3) 50 pts –

20 pts – factoring n into primes p and q via Pollard Rho
10 pts – finding d via Mod Inverse Call
10 pts – using d to get plaintext in numbers
10 pts – converting numbers of plaintext to letters

- 4) 30 pts –

15 pts – finding the secret key used for decryption (a for loop is good enough, the
Optimized algorithm is not required for full credit. It should run in a few
Seconds anyway.)
15 pts – Using the decryption key to get plaintext; 10 pts to go to numbers, 5 pts to go
from the numbers to letters.