

## Fall 2025 CIS 3362 Homework #6 Grading Criteria

1) 10 pts total (3 pts A to B, 3 pts B to A, 4 pts shared)

- 2 pts for showing Alice sends Bob  $23^{83} \bmod 97$ , 1 pt for the result (ok to use IDLE)
- 2 pts for showing Bob sends Alice  $23^{65} \bmod 97$ , 1 pt for the result
- 2 pts for showing either shared key expression ( $57^{65}$  or  $29^{83} \bmod 97$ ), 2 pts for the result

2) 10 pts total

- 1 pt –  $n$ ,  $\phi(n)$
- 2 pts – Euclidean Alg
- 6 pts – Extended Euclidean, steps should be written
- 1 pt – Extracting the answer

3) 50 pts total

- 10 pts total for a clear description of how they factored  $n$ .
- 5 pts for using the factorization of  $n$  and computing tools to figure out  $d$ .
- 10 pts for using the value of  $d$  and computing tools to get the numeric decryption
- 25 pts for converting that numeric decryption into valid Radix-64 readable plaintext.

Note: feel free to give some partial credit based on their write up for any part, especially the last one.

4) 30 pts total

10 pts to solve the Discrete Log problem to get the private key – definitely pay attention to if they used the divide and conquer or the slow method, note how long the slow method took (I am curious...)

10 pts to decrypt the numerical ciphertext to numerical plaintext

10 pts to convert the numerical plaintext to the actual characters (mod div 26...)

Note: feel free to give some partial credit based on their write up for any part