SCI 2000
Introduction to Encryption, Assignment 4
Due March 29 via upload to Crowdmark.

Questions will be marked both on correctness and clarity of presentation. Poor writing and sloppy/illegible presentation both impact the clarity of your work and so will be penalized. For this assignment, you can use Wolfram Alpha (https://www.wolframalpha.com/) to perform computations, however you must show all steps in your computations to get credit.

Question 1: I am of the opinion that you should get credit for the effort you put into transitioning to an online-only platform. For this question, the answer is your name and student number written on a piece of paper. Literally write your name and student number on a piece of paper, figure out how to use crowdmark to upload your answer, and you get the points.

Question 2: My public key is $(127, 899)$. Encrypt the last message 337 so that it is ready to send

to me. When computing the large power necessary for this question, show all the steps covered in our class on fast exponentiation by repeat squares: Write the exponent in binary, create a table of powers where the exponent is 2^k, use the properties of exponents to calculate the final answer as a product of entries from the table.

Question 3: With my public key as in the last question, you observe someone sending me the encrypted message 388. Break their encrypted message by taking my public key $(e, n) = (127, 899)$ and computing $\phi(n)$ and using this to find my private key (d, n). Again, show all steps (even though I know you are using Wolfram Alpha for computations).

Question 4: Find a Fermat witness for the number 77. What percentage of numbers m with $1 \leq m \leq 77$ are Fermat witnesses for 77?