Group 6 Grade – Graded by Group 2

Problem 2.6

The answer is correct and very well done. They clearly work out their problem and effectively convey how they got their answer.

Problem 2.8

All the answer for this problem all look correct. Again, they worked out their solutions well and demonstrated their knowledge of the material.

Problem 2.17

1137 = 21 (mod 71)

CORRECT

15659 = 116 (mod 593)

CORRECT

650319 = 2213 (mod 3571)

CORRECT

The program created for this question solves the discrete logarithm problem by utilizing Shanks’ baby-step giant-step algorithm and Fermat’s little theorem. The program always outputs a correct answer, and a set of inputs that would print an incorrect solution was unable to be found. The program was written in Python which can handle very large numbers, so there will be no issues with large numbers being rounded incorrectly.

Overall, Group 6 did very well on this assignment and deserve an A on it.