CRYPTOGRAPHY MISSION 05 SOLUTIONS

Deadline: Thursday, 6 October 2016 at 3:05pm
This mission covers Sections 3.4, 3.6, and current issues.

1. Graded Problems

1. (Fermat's Little Theorem and Euler's Theorem) Compute each of the following without the aid of a calculator or computer (you can double-check with some code though).
   a. $\varphi(35)$

24

   b. $514^{372} \mod 13$

$(514^{12})^{31} \mod 13 \equiv 1^{31} \mod 13 \equiv 1 \mod 13$

   c. $2^{49} \mod 15$

$(2^8)^6)(2) \mod 15 \equiv 1^6(2) \mod 15 \equiv 2 \mod 15$