Introduction to Cryptography (462)
Homework 07
T.J. Borrelli
Due: Thursday, November 30th, 2017 at 2pm

- Be sure to put your NAME and Section number on the first page.
- If you upload your submission to the myCourses dropbox, I will only accept .pdf format and only the last thing you submit will be accepted.
- This homework is related to Chapter 7 in the Paar and Pelzl (P&P) book and notes.
- This is the last graded hw.
- **For each question, show the details of your computation unless otherwise specified.**

1. Encrypt and decrypt by means of the RSA algorithm with the following system parameters:

   (a) $p = 3, q = 11, d = 7, x = 5$

   (b) $p = 5, q = 11, e = 3, x = 9$

2. Consider moduli 11 and 13 in the Chinese Remainder Theorem. What numbers are represented by the pairs (1,0), (4,5) and (5,4)? Show the details of your work.

3. Find two non-standard roots (not 1, nor -1) of $\sqrt{1}$ in $\mathbb{Z}_{77}$.

4. Use your favorite programming language to implement the Fermat Primality Test. (Note: your program should use the Square-and-Multiply algorithm from last time.)

   Use your program to find the last three Carmichael numbers less than 10^6 and the last three Carmichael numbers less than 10^7.

   Submit your code in the PDF file as usual.