MACM 442/MATH 742/MATH 800
Assignment 4, Fall 2008

Michael Monagan

This assignment is to be handed in on Tuesday October 28th at the beginning of class.
Late penalty: 20% off for up to 24 hours late, zero after that.

Chapter 5 exercise 5.14, 5.17, 5.34.
Chapter 6 exercises 6.1, 6.3, 6.6, 6.9, 6.10, 6.11.

For exercise 5.17 include an example to illustrate how you compute x from y_1, y_2 and y_3.

For exercise 6.1 use the `sort` command in Maple. See `?sort`.
Note, Maple is using "mergesort" which does $O(n \log n)$ comparisons in the worst case.

For exercise 6.9, decrypting the first 6 lines (24 characters) of the ciphertext is enough.

For exercise 6.11 (a), (b) and (c) use the appropriate Maple commands.
Note, the `Powmod(...) mod p` command in Maple implements the square-and-multiply algorithm. Using the `Rem(...) mod p` command, program your own version of the square-and-multiply algorithm to compute x^{25} in the given field.

Additonal exercises.

1: Suppose Bob is using the Rabin cryptosystem with $p = 103$, $q = 107$ hence $n = 11021$. Suppose Alice computes $y = x^2 \bmod n$ and sends y to Bob. If $y = 10990$ what are the four possible values x can be? Apply the Chinese remainder theorem to solve this. Show your working.

2: Using the `nextprime` and `isprime` commands in Maple, find the first prime $p > 10^{100}$ of the form $p = 2q + 1$ where q is also prime. Now show that 2 is a primitive element and 3 is NOT a primitive element in $\mathbb{Z}_p$. What is the order of 3 in $\mathbb{Z}_p$?

3: (for graduate students)
Implement algorithm 5.13 on page 217. Test it on the authors' data (n=1457, b=779, y = 772) and generate the numbers in Figure 5.3 on page 218.