MACM 442/MATH 742/MATH 800
Assignment 1, Fall 2008

Michael Monagan

Due Tuesday September 16th, 10:30am, at the beginning of class.
Late penalty: -20% for up to 24 hours late, zero after 24 hours late.

Chapter 1

Exercises 1.7, 1.9, 1.11(b), 1.13, 1.16, and 1.21.

Notes on exercises.
For 1.9, 1.11(b), and 1.13 please use Maple to compute the answers.
You will probably find that you will spend more time on problem 1.21 than all the other problems on this assignment put together and so it will be worth more marks. It is also the question which is the most fun. Note that the plaintext for one of the problems is not English.

Additional questions for all students:

1: Oscar knows that the plaintext "SELLIT" when encrypted with the Hill Cipher that Alice is using yields the ciphertext "GCGJFA" (using the encoding A=0, B=1, C=2, ..., Z=25). If Oscar also knows that $m = 2$, does he have enough information to determine the key uniquely? If so, what is it? If not, what keys, if any, are possible?

2: Table 1.4 on page 35 lists values for M_g for the ciphertext in Example 1.12 on page 34 which begins CHREEVO.... Write a program that reproduces the the numbers in row 2 of the table, i.e. the numbers 0.069, 0.044, 0.032, etc.