MACM 442/CMPT 881/MATH 800
Assignment 2, Fall 2006

Michael Monagan

This assignment is to be handed in on Thursday October 5th at the beginning of class.
Late penalty: 10% off for each day late.

Q1: Below are permutations for two 4-bit S-boxes. They are permutations of the numbers 0, 1, 2, ..., 15. One is a linear function of the vectors 0000, 0001, ..., 1111 and the other is not. For the linear one, find the matrix A and vector b s.t. $S(x) = Ax + b$. For the non-linear one, prove that it is non-linear.

```
 3   1   7   5  10   8  14  12  2  0  6   4  11   9  15  13
 9  14  15   5   2   8  12   3  7  0  4  10   1  13  11   6
```

Q2: Implement algorithm 3.1 SPN($x, \pi_S, \pi_P, K^1, K^2, ..., K^{N+1}$). Test your algorithm by using it to check the example on page 77 with x = 0010011010110111. You should get y = 1011110011010110. Please print out also the intermediate values of u, v, w. Note, I suggest you use lists to represent a vector of bits. If w and k are two lists in Maple then you can add them mod 2 directly using $w + k$ mod 2 in Maple.

Q3: Implement the square and multiply algorithm. Use either Algorithm 5.5 or the algorithm I gave in class. Show that it is working by computing 2^{43} mod 35.

Conventional wisdom says that the primes used for the RSA cryptosystem should be 100 decimal digits or larger - some implementations are now using 154 digit primes (512 bits). Use Maple to create two random 154 digit primes p and q (using the `nextprime` command) and compute $n = pq$. Choose a suitable encryption exponent b (do this with care) then compute the decryption exponent a. Choose an integer x at random from $\mathbb{Z}_n$ for the plaintext. Use your square and multiply algorithm to compute $y = x^b$ mod n and y^a mod n.

Chapter 5 exercises 5.3(a), 5.6, 5.8, 5.10, 5.12, 5.15.
For problem 5.3 execute the extended Euclidean algorithm by hand.
For exercise 5.12 decrypt the first 5 rows of Table 5.1 only.