MACM 498/CMPT 881/MATH 800
Assignment 2, Fall 2004

Michael Monagan

This assignment is to be handed in on Thursday October 7th at the beginning of class. Late penalty: 10% off for each day late.

Q1: Consider the linear recurrence $z_{i+4} = z_i + c_1 z_{i+1} + c_2 z_{i+2} + c_3 z_{i+3} \bmod 2$. For all choices of c_1, c_2, c_3 determine the period π of the recurrence using initial values $z_1\, z_2\, z_3\, z_4 = 1011$.

Q2: 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. Find out which is which (show your working). For linear one, give the matrix A and vector b s.t. $S(x) = Ax + b$.

```
 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
```

Q3: 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 $y = 1011110011010110$. The SPN function as stated cannot be inverted as suggested in exercise 3.1. Modify the key schedule so that you can use your SPN function to decrypt y (and check that you get back x). You will need π_S^{-1} and π_P^{-1}. The permutation π_P used in this example has a special property. What is it? Hint: look at π_P^{-1}.

Q4: Implement the square and multiply algorithm. Show that it is working by computing $2^{43} \bmod 35$. 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 100 digit primes p and q (using the `nextprime` command) and compute $n = pq$. Choose a suitable encryption exponent b and compute the decryption exponent a. Choose an integer x at random from $\mathbb{Z}_n$ for the plaintext. Use your square and multiply algborithm to compute $y = x^b \bmod n$ and then $y^a \bmod n$.

Chapter 5 exercises 5.3(a), 5.6, 5.8, 5.10, 5.12.
For problem 5.3 execute the extended Euclidean algorithm by hand.
For exercise 5.12 just decrypt the first 8 rows of Table 5.1.

Computing 881 and Math 800 students should also do exercise 5.13. For parts (b) and (c) decrypt the number y from Question 4 above (based on the 100 digit primes). Time the decryption (using the `time()` command in Maple). Is it really 4 times faster?