MACM 442/MATH 742/MATH 800
Assignment 2, Fall 2008

Michael Monagan

This assignment is to be handed in on Tuesday September 30th at the beginning of class. Late penalty: -20% for up to 24 hours late, zero after that.

Q1: Suppose we use the One-Time-Pad to encrypt one bit with key $K \in 0, 1$. Show that if the $\Pr(K = 0) \neq 1/2$ then the One-Time-Pad does NOT have perfect secrecy.

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. 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
```

Q3 (exercise 3.1). Let y be the output of Algorithm 3.1 on input x

$$y = \mathrm{SPN}(x, \pi, S, K^1, K^2, ..., K^{N+1})$$

where π is a permutation, S is a substitution, and $(K^1, ..., K^{N+1})$ is the key schedule. Determine how to use the same algorithm to invert y, i.e. what do $(L^{N+1}, L^N, ..., L^1)$ need to be so that

$$\mathrm{SPN}(y, \pi^{-1}, S^{-1}, L^{N+1}, L^N, ..., L^1) \ = \ x \ ?$$

Q4: Implement algorithm 3.1 $\mathrm{SPN}(x, S, P, K^1, K^2, ..., K^{N+1})$. 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. Check that your answer to Q2 is correct by inverting y to get x.

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.