Date: Wednesday, February 13, 2002
Lecturer: Dr Jean-Yves Chouinard
Office: Colonel-By Hall, room A-610

ELG-5373 Secure Communications and Data Encryption

Assignment #2 (due on Wednesday, February 27, 2002 at the beginning of the lecture.)

Question 1: *(permutation)*

Let $\prod(m)$ be a permutation of the n-bit integers: $0, 1, \ldots, 2^n - 1$, where $0 \leq m \leq 2^n$. For instance, the standard permutation P in the DES algorithm is a permutation for 32-bit integers. If $\prod(m) = m$ then this value of m is called a fixed point in the permutation.

a) Find an expression for the probability $P_{\text{no fixed point}}$ as a function of $N = 2^n$. *Hint:* Consider the set of permutations S_N on $[0, \ldots, 2^n - 1]$.

b) Show that more than 60% of the mappings will have at least one fixed point.

Question 2: *(DES modes of operation)*

Problem 3.4 from the course notes.

Question 3: *(double DES)*

Consider double DES encryption with keys K_1 and K_2: $C = DES_{K_2}\left[DES_{K_1}(M)\right]$. If $DES_{K_2}(X) = DES_{K_1}^{-1}(X)$, then K_1 and K_2 are called *dual keys*. This undesirable since the ciphertext C will be the original plaintext M. Now a key K will be a *self-dual key* if it is its own dual key.

a) Show that if C_0 is either all 0's or all 1's and D_0 is either all 0's or all 1's, then the key K is a self-dual key.

b) Show that the following keys (in hexadecimal form) are self-dual:

$K_1 =$	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$K_2 =$	F	E	F	E	F	E	F	E	F	E	F	E	F	E	F	E
$K_3 =$	1	F	1	F	1	F	1	F	0	E	0	E	0	E	0	E
$K_4 =$	E	0	E	0	E	0	E	0	F	1	F	1	F	1	F	1

c) Show that the following pairs of keys are dual:

$K_{1,1} =$	E	0	0	1	E	0	0	1	F	1	0	1	F	1	0	1
and $K_{1,2} =$	0	1	E	0	0	1	E	0	0	1	F	1	0	1	F	1
$K_{2,1} =$	F	E	1	F	F	E	1	F	F	E	0	E	F	E	0	E
and $K_{2,2} =$	1	F	F	E	1	F	F	E	0	E	F	E	0	E	F	E
$K_{3,1} =$	E	0	1	F	E	0	1	F	F	1	0	E	F	1	0	E
and $K_{3,2} =$	1	F	E	0	1	F	E	0	0	E	F	1	0	E	F	1

Question 4: *(linear cryptanalysis of DES)*

We have seen that DES linear cryptanalysis exploits the sometimes biased input-output relationship of a given substitution box. Give the input-output relationship of substitution boxes S_4 and S_7. Which one is better against linear cryptanalysis? How do S_4 and S_7 compare to S_5 (section 3.6.2 of the course notes). Justify your answers (e.g. tables).