T-79.5501 Cryptology
Midterm Exam 1
Friday, February 21, 2014

1. (6 pts) Let n be a positive integer. A *Latin square* of order n is a $n \times n$ array L of the integers $1, 2, \ldots, n$ such that every one of the n integers occurs exactly once in each row and each column of L. We denote by $L(i, j)$ the element in the i'th row and j'th column of L.

   An example of a Latin square of order 3 is as follows.

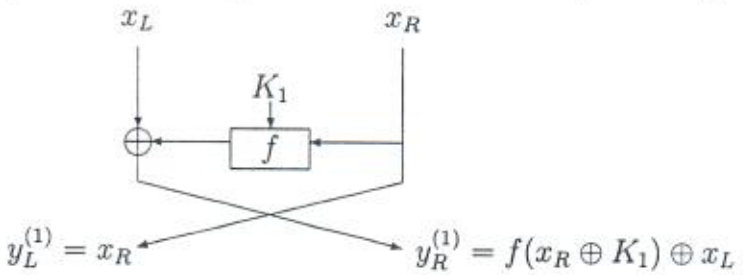
1	2	3
3	1	2
2	3	1

   Given any Latin square L of order n, we can define a cryptosystem where $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{1, 2, \ldots, n\}$, and

   $$e_i(j) = L(i, j), \text{ for all } i \in \mathcal{K} \text{ and } j \in \mathcal{P}.$$

   Prove that this *Latin Square Cryptosystem* achieves perfect secrecy if every key is used with equal probability.

2. (6 pts) Let us consider impossible differentials over a five-round Feistel cipher with a bijective round function f and a fixed key. One round of such a cipher is depicted below.



   Let us assume that the difference in the right half of the inputs x_R is equal to zero, and the difference in the left half of the output $y_L^{(5)}$ of the 5-round Feistel cipher is equal to zero. Show that then a non-zero difference in the left half of the input x_L can never be equal to the difference in the right half $y_R^{(5)}$ of the output.

3. (6 pts)Let us consider the Boolean function $f(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_3$. Compute the correlations $c(f, L_w)$ for all $w = (w_1, w_2, w_3) \in \mathbb{Z}_2^3$.

4. Let us consider the function $g : \mathbb{Z}_{16} \to \mathbb{Z}_{16}$ defined as

   $$g(x) \quad = \quad (5^x \bmod 17) - 1, \text{ for } x \in \mathbb{Z}_{16}.$$

   By identifying $u = u_4 2^3 + u_3 2^2 + u_2 2 + u_1 \in \mathbb{Z}_{16}$ with $(u_4, u_3, u_2, u_1) \in \{0, 1\}^4$, the function g is defined from $\{0, 1\}^4$ to $\{0, 1\}^4$. Now consider the least significant bit of the output $g(x)$ and denote it by $f(x)$. Then f is a Boolean function of four variables.

   (a) (2 pts) Compute the truth table of f.

   (b) (2 pts) Compute the algebraic normal form ANF of f.

   (c) (2 pts) Compute the correlation between $f(x)$ and x_4, which is the most significant bit of x.

Exam Calculator Policy. It is allowed to use a function calculator, however no programmable calculator.