Advanced Topics in Cryptography – Midterm Test

June 13, 2012

Question 1

For $n \in \mathbb{Z}^+$, a Latin square of order n is defined as $L \in \mathbb{Z}^{n \times n}$ such that every one of the n integers occurs exactly once in each row and each columns of L. An example of a Latin square of order 4 is as follows:

3	1	4	2
1	2	3	4
2	4	1	3
4	3	2	1

Given any Latin square of order, define the *Latin Square Cryptosystem* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ as follows: $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{1, \ldots, n\}$. For $1 \leq i \leq n$, the encryption rules are defined as $e_i(j) = L(i, j)$. Therefore, each row of L defines an encryption rule. For example, given the key $K = 1$, we take the 1st row and then we encrypt the plaintext $x = 3$ (corresponding to the 3rd column) as the ciphertext $y = 4$, since $e_1(3) = L(1, 3) = 4$.

Give a direct proof that this cryptosystem has perfect secrecy for any n, if every key is used with equal probability.

Question 2

Compute the deception probabilities for impersonation attack P_{imp} and for substitution attack P_{sub} for the authentication code defined by the following authentication matrix:

key \ x	1	2	3	4
1	1	1	2	3
2	1	2	3	1
3	2	1	3	1
4	2	3	1	2
5	3	2	1	3
6	3	3	2	1

Question 3

Prove that a cryptosystem is perfectly secure if and only if $H(P|C) = H(P)$, where P and C are the random variables describing a plaintext and a ciphertext, respectively.

Question 4

Let X, Y and Z be random variables.

Give a direct proof that $H(X, Y|Z) = H(X|Z) + H(Y|X, Z)$.

Question 5

Let X be a random variable taking values in a finite set $\mathcal{X}$.

Prove that $H_2(X) \leq H(X)$, with equality if X is uniform over $\mathcal{X}$.