**Applied Cryptography**

**MSIS-11 (Fall 2012)**

**Assignment #1**

Issue Date: 11 Oct 2012

Due Date: 26 Oct 2012 (before start of class)

Note: The solution to this assignment should be written in hand with ink/ball point pen (no pencil). However, any part of the assignment done programmatically on computer can be submitted in printed form. Late submissions will not be accepted.

**Question #1**

Have a look at the substitution cipher and recall the definition of perfect secrecy. Prove that the substitution cipher is perfectly secure for the special case of ℓ = 1, and that it it is not perfectly secure if ℓ ≥ 2.

**Question #2**

**Question #3**

Exercise 1.5 of the text book “CRYPTOGRAPHY – Theory & Practice” by Stinson

**Question #4**

Exercise 1.11 of the text book “CRYPTOGRAPHY – Theory & Practice” by Stinson

**Question #5**

**Question #5**