**Applied Cryptography**

**MSIS-11 (Fall 2012)**

**Assignment #1**

Issue Date: 20 Sep 2012

Due Date: 27 Sep 2012 (before start of class)

Note: The solution to this assignment should be written in hand with ink/ball point pen (no pencil). Late submissions will not be accepted.

**Question #1**

Exercise 1.1 of the text book “CRYPTOGRAPHY – Theory & Practice” by Stinson

**Question #2**

Cryptanalyze the following ciphertext using Kasiski and index of coincidence methods.



**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**

Please state the key space of the following ciphers. Also state the time required for a brute force attack (i.e., exhaustive search for the key) if 10^6 searches can be done per second.

1. Substitution cipher (26 English alphabets and 10 numeric digits)
2. Affine Cipher if extended ASCII characters (8-bit values) are used as input and output characters. (You may use modulus 257)

**Question #5**

Comment and compare the search effort for the key in case of substitution cipher, vigenere cipher, affine cipher and Hill cipher once a plaintext and corresponding ciphertext pair is available to the attacker.