Assignment: 3 **Cryptography** **Due date: 27-11-2019**

Q:1: Answer the following. (Not more than three lines)

a) Why DES requires an even number of iterations?
b) Why we do not mix the columns in the last round of AES?
c) What if we mix the columns in last round and use AES as irreversible algorithm?
d) What if, we do not use ASCII in symmetric key cryptography? Will it be convenient? Why OR why not?
e) Why we follow standards for encryption? What if we design our own standards?
f) Can we use Asymmetric key for symmetric algorithm? Why OR why not?

Q:2: A message was encrypted using Advanced Encryption Standard, which is classified due to some security reasons. After two weeks, it is disclosed but we only have a Key and a Cipher text. You are advised to find the plain text by inverse AES algorithm. (Decrypt the message)

Key: Thats my Kung Fu

Cipher Text: 29 C3 50 5F 57 14 20 F6 40 22 99 B3 1A 02 D7 3A

Q:3: What if we apply "Safe primes" instead of prime values for P and Q in RSA algorithm? Use an example by your own P and Q and briefly explain. (Text answer must be not more than five sentences.)

Section (B)

Q:4: Iterate the quadratic equation for 256 elements of a unique string (0-255) elements. Design a (16x16) Substitution Box and give a Stem(plot) of all your entries. We require flowing properties:

a) S-Box must be unique.
b) No two students can design a single S-Box.
c) We require three different fixed values as well as different Seeds.
d) Keep remember! You are bound to design it only by a Quadratic Equation i.e.

$$aX_{(i)}^{2} + bX_{(i)} + C = X_{(i+1)}$$