**PSG COLLEGE OF TECHNOLOGY**

**DEPARTMENT OF APPLIED MATHEMATICS AND COMPUTATIONAL SCIENCES**

**M. Sc. Software Systems - COMPUTER NETWORKS AND TCP/IP LAB**

**4th Semester**

**PROBLEM SHEET - 1 – Encryption and Decryption**

The purpose of this lab assignment is to gain familiarity with encryption and decryption procedures employed in Network communications. Write a program in Python for performing encryption and decryption of a file.

**Tasks to be performed:**

1. A Client program will read data from File A, perform encryption and write the encrypted data to File B.
2. A Server program will read from File B, decrypt the data and write the data to File C.
3. Phase 1: Use substitution or transposition ciphers for performing encryption/decryption
4. Phase 2: Use AES-256 by using appropriate python module/library.

**Links for reference:**

<http://www.crypto-it.net/eng/simple/substitution-ciphers.html>

http://www.crypto-it.net/eng/simple/transposition-ciphers.html