300128 - Information Security

Tutorial and Lab Practice - Week Three (follows lecture 2 & 3)
This work will not be marked, it should be completed within one week

Read text book and lecture notes, review the terminology introduced

Reading chapters:

- Chap4.1 Traditional block cipher structure
- Chap4.2 The Data Encryption Standard
- Chap4.4 The strength of DES
- S-DES functions

Tutorial

1. Encrypt the plaintext "CYBER INTELLIGENCE" by using the following ciphers.
   [i] Vigenere Cipher with a key "BOMB".
   [ii] Playfair Cipher with "SECURITY" as the keyword.
   [iii] Transposition Techniques (refer to note P31, lecture 2) with a key=4213.
2. Encrypt "OZ" with Hill Cipher by the key K_{11}=3, K_{12}=2, K_{21}=5, K_{22}=9.
3. A binary string 101010011011 is encrypted to 110010010111 by exclusive OR operation. Find out the key string.

Lab Practice

1. Write a program to count the letter frequencies of a file. The file can be entered either by the keyboard, or by reading a pre-defined file.