300128 - Information Security

Tutorial and Lab Practice - Week Four (follows lecture 3 & 4)
This work will be marked in Week Six during lab. session **(4%)**

Read text book and lecture notes, the DES system, modular arithmetic and the terminology introduced

Reading chapters:

- Chap2.1 Divisibility and The Division algorithm
- Chap2.2 The Euclidean algorithm
- Chap2.3 Modular arithmetic

Tutorial

1. A permutation function P is defined as 7351624. Find the result by applying P^{-1} on string "methods". **(1%)**
2. In a S-DES system, If 1010, 1100, 0011 input to S1, find out the outputs.
3. If 1010101010 are the input to S-DES key generator, find out the keys. **(1%)**
4. In a DES system, a S-Box consists of 8 sub S-Box. For each sub S-Box, the input is 6 bits and output is 4 bits. Use S1 on P31 of lecture note three, find out the corresponding output bits if the inputs are B1=101010, B2=100011, B3=011000 and B4=001001 **(1%)**
5. For the P function defined on P29 lecture note three, find out P^{-1}.
6. Using the P function defined on P29 lecture note three, find out the output string for input 11100101000011110010001101010100.**(1%)**

Lab Practice

1. Write a program to implement the Playfair Cipher with "risk" as the key word. Then test your program with plaintext "playfair cipher".