300128 - Information Security

Tutorial and Lab Practice - Week Six (follows lecture 5 & 6)
This work will be marked in Week Eight during lab. session **(4%)**

Read text book and lecture notes. Review finite fields and the terminology introduced

Reading chapters:

- Chap5.1 Groups
- Chap5.2 Rings
- Chap5.3 Fields
- Chap5.4 Finite field of the form

Tutorial

1. Show that the set Z_n = {0, 1, 2, ..., n-1}, with arithmetic + operation modulo n is an abelian group. Also show that the same set with arithmetic +,X operations modulo n, is a field when n is a prime number. **(1%)**
2. Is the set of nonzero real numbers under multiplication an abelian group? Justify your answer. **(1%)**
3. Is the set of all integers under arithmetic addition and multiplication an integral domain? Justify your answer.
4. Compute 3^{23} mod 5 by using modular arithmetic. List the steps. **(1%)**
5. S_4 is a group of all permutations of 4 distinct symbols. List all the elements of S_4. Is S_4 an abelian group? Use an example to explain. **(1%)**
6. $\phi(25)$ refers to the positive integers less than 25 and relatively prime to 25. List these integers.
7. RSA encryption algorithm:
   Given:
   Two prime numbers: p=11 and q=3
   The message to be sent is: M=6
   The public key is: e=7
   (i) Find out the corresponding secret key d.
   (ii) Compute the cipher text C.

Lab Practice

1. Write a program to calculate Euler's totient function ϕ(n).