300128 - Information Security

Tutorial and Lab Practice - Week Five (follows lecture 4 & 5)
This work will not be marked, it should be completed within one week

Read text book and lecture notes. Review modular arithmetic, and the terminology introduced

Reading chapters:

- Chap2.4 Prime numbers
- Chap5.1 Groups
- Chap5.2 Rings
- Chap5.3 Fields
- Chap5.4 Finite Field of The Form

Tutorial

1. Compute the greatest common divisor of 13 and 104 using Euclid's algorithm by listing each of the steps.
2. Compute the multiplicative inverse of 9 under modulo 31 using the extended Euclid's algorithm by listing each of the steps.
3. Compute additive and multiplicative inverses of 7 and 9 in Z_{11} (mod 11).
4. Find out whether or not 4 and 7 have multiplicative inverse in Z_{14} (mod 14).
5. Let S be the set of even integers under the operations of addition and multiplication. Is S a ring? Is it commutative? Is it a field? Justify your answer.
6. Find out whether or not the integer pairs are relatively prime: (8, 15), (6, 50), (3, 31) and (3, 21).
7. Is the set of all real numbers under the arithmetic addition and multiplication a field? Justify your answer.
8. Consider a set S={a,b} with addition and multiplication defined by: a+a=a, a+b=b, b+a=b, b+b=a, axa=a, axb=a, bxa=a, bxb=b. Is S a ring? Justify your answer.

Lab Practice

1. Write a program to implement the Euclid's algorithm.