300128 - Information Security

Tutorial and Lab Practice - Week Seven (follows lecture 6, 7)
This work will not be marked, it should be completed within one week.

Read text book and lecture notes. Review finite fields, public key encryption/decryption, digital signature, blind signature and the terminology introduced

Reading chapters:

- Chap9.1 Principles of public key cryptosystems
- Chap9.2 The RSA algorithm
- Chap10.1 Diffie-Hellman key exchange

Tutorial

1. 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 field? Justify your answer.
2. For each of the following equations, find an integer x that satisfies the equation.
   7x (mod 3) = (5 mod 3)
   x/20(mod 5) = (7 mod 4)
3. Sign message 2 with RSA Digital Signature. Assume p=5, q=7. Then verify the signature (you may use a calculator).
4. In Diffie-Hellman key exchange scheme, given p=11,
   (i) find out its primitive root. Is the primitive root unique?
   (ii) given X_A is 3 and X_B is 4, find out the key.
5. Use Fermat's Theorem compute 2^6 mod 7, 97^{130} mod 131 and 51^{22} mod 23.

Lab Practice

1. Write a program to implement the square and multiply algorithm (refer to P18, lecture 5) to compute a^b mod n.