300128 - Information Security

Tutorial and Lab Practice - Week Nine (follows lecture 8, 9)
This work will not be marked, it should be completed within one week

Read text book and lecture notes. Review key distribution, message authentication and the terminology introduced

Reading chapters:

- Chap12.1 Message authentication requirements

- Chap12.2 Message authentication functions

Tutorial

1. What is a public key certificate? What does the certificate contain?

2. Write a detailed key distribution protocol (as lecture7, P7 shows) for model 2 (on P12 of lecture7). Assume mutual authentication of A and B is needed. Before this protocol can be carried out, which key needs to be distributed? Why?

3. Alice and Bob share a permanent secret key K_{ab}. They want to securely communicate with a session key K_s. Write a protocol with proper assumption for the session key distribution that meets the following requirements:

   (a) Confidentiality

   (b) Freshness

   (c) Authentication

4. Assume that you only have symmetric key capacity and wish to send a secret message to your communication partner. Design a protocol to achieve this.

5. Assume that you only have public key capacity and wish to send a secret message to your communication partner. Design a protocol to achieve this.

Lab Practice

1. Write a program to implement the Square and multiply algorithm used in RSA system. Your program must allow user input. The input power can be binary or decimal.