300128 - Information Security

Tutorial and Lab Practice - Week Ten (follows lecture in week 9, 10)
This work will be marked in Week Twelve during lab. session **(4%)**

Read text book and lecture notes. Review user authentication, Kerberos and the terminology introduced

Reading chapters:

- Chap15.1 Remote user authentication principles
- Chap15.2 Remote user authentication using symmetric encryption
- Chap15.3 Kerberos
- Chap15.4 Remote user authentication using asymmetric encryption

Tutorial

1. Improve the security of the protocol for key distribution and management on P16 of lecture 7 by encrypting every message transmitted in the protocol using existing resource (keys) **(1%)**. Before the protocol can be carried out, what kind of key distribution should be performed? **(1%)**
2. In the message authentication protocol on P15 of Chapter 8, there are two rounds of encryption involved, what's the purpose of each of the encryption? **(1%)**
3. What kind of requirements need to be achieved for massage authentication? What kind of methods are normally used to achieve such requirements?
4. Study the message authentication protocol on P14 of lecture 8, then convert it by public key encryption. You need to make proper assumption. **(1%)**
5. The following user authentication protocol is based on symmetric keys:
   1: $C \rightarrow AS$: ID_c, P_c, ID_v
   2: $AS \rightarrow C$: Ticket
   3: $C \rightarrow V$: ID_c, Ticket

   Ticket = $E_{kv}[ID_c, AD_c, ID_v]$
   Convert this protocol to one which is based on pure public key system. You need to make proper assumption.
6. In the previous protocol, if the first step is as follows:
   1: $C \rightarrow AS$: ID_c, P_c
   Does it work? Why?

Lab Practice

1. Write a program using the extended Euclidean algorithm to find the multiplicative inverse of a mod n. Your program should allow user to enter a and n.