# 300128 - Information Security

*Tutorial and Lab Practice - Week Eight (follows lecture 6, 7 & 8)*
*This will be marked in Week Ten during lab. session* **(4%)**

**Read text book and lecture notes. Review digital signature, blind signature, key distribution and the terminology introduced**

**Reading chapters:**

- Chap14.1 Symmetric key distribution using symmetric encryption
- Chap14.2 Symmetric key distribution using asymmetric encryption
- Chap14.3 Distribution of public keys
- Chap14.4 X.509 Certificates 459

## Tutorial

1. In RSA blind signature, can the blinding factor R be any value? Explain the reason.
2. x and y are positive integers. If (x+3) mod 7 = 2 and 5y mod 11 = 3, find out x, y. Are they unique? **(1%)**
3. Is 3 a primitive root of 7? Justify your answer. **(1%)**
4. RSA blind signature algorithm: Given: (you may use a calculator).
   Two prime numbers: p=11 and q=3
   The message to be signed is: M=6
   The public key is: e=7

   (i) List all the possible candidates of the blinding factor R.
   (ii) If the chosen R is 2, find out $\mathrm{R}^{-1}$.**(1%)**
   (iii) Calculate the signature with blinding factor S'. **(1%)**
   (iv) Calculate the signature with the blinding factor filtered out S.
5. A hash function is also called a compression function, why? Do we need to reverse the hash function?
6. What is a session key? How long is its life time?

## Lab Practice

1. Write a program to tell if a given number is a prime number. If it is, find out one of its primitive root.