# IY5502 Introduction to Cryptography and Security Mechanisms

## Assignment 1

## Strictly Due: Wednesday 24th October 2012 13.00

**Q1** Explain the difference between symmetric cryptography and public-key cryptography, including in your answer reference to the main key management challenges for each of them. [5]

**Q2** A government department decides that it needs to use encryption to protect communication between itself and its international counterparts. At a meeting with its counterparts it is decided to develop a proprietary encryption algorithm for this purpose.

a) Is this decision justifiable? [2]
b) What risks and problems do they potentially face? [5]

**Q3** The one-time pad provides perfect secrecy, at a cost.

a) Provide an example of an application where it might be reasonable to use a one-time pad, explaining why the various key management costs normally associated with use of the one-time pad are ``justifiable'' for your application. [4]
b) Draw a square look-up table which demonstrates that using the Vernam Cipher to encrypt three bits of plaintext results in a one-time pad based on a Latin Square. [3]

**Q4** Stream ciphers can be argued to be the ``poor person's one-time pad''.

a) In what ways is a stream cipher similar to the Vernam Cipher? [2]
b) In what ways is a stream cipher more practical to implement than a Vernam Cipher? [4]

**Total marks 25** **KMM**