CS 5311 Assignment 1

Due on Thursday, Feb. 31, 2013

Each student is required to do this assignment **individually** and to hand in a hard copy of your solution on due date. Computer typeset for the solution is preferred. Hand written is also acceptable, but request to write clearly. If you use computer to solve some questions, you don't need to include the computer program, but just put the answer (results) in your solution.

Put your Name, Student Number, Course Number (CS 5311) on your answer sheet.

Assignments which are not met the above requirements will not be marked. The score of the assignment will depend on:

Specification and documentation: 10 %

Correctness: 90 %

Late assignments will be penalized and will not be accepted after 3 days.

Problem 1.

Prove Theorem 1.1.8: "There exists orthogonal latin squares of order n, if $n \not\equiv 2 \bmod 4$" using previous Theorems of the lecture notes.

Problem 2.

Construct 6 MOLS(7) and then give an OA$(8, 7)$ based on the MOLS.

Problem 3.

Use the Gilbert-Varshamov Bound to prove that the following orthogonal arrays exist:

1. a 4-(2,9,8)-OA;
2. a 4-(2,12,16)-OA;
3. a 3-(3,10,9)-OA.

Problem 4.

Using the OA$(8, 7)$ in Problem 2 to construct an authentication code with 8 source states and 7 authenticators. Suppose Alice and Bob chose the key $K = 10$. If Alice wants to send the source state 5 to Bob, what is the authenticator? If Alice wants to send Bob the source state 6, what is the authenticator? If Alice use the same key to authenticate both source states, how can the Oscar figure out the secret key used by Alice and Bob?