

MAS 790 Graduate Seminar – Discrete Mathematics I Course Information

Recommended Reading Stinson, Douglas R. **Combinatorial designs : constructions and analysis**, Springer, 2004

Grading policies

Presentation: 50%

Mini Report Writing: 50%

Course Outline

The objective of this course is to study some combinatorial techniques as well as their ingenious applications, a focus will be on the design theory and its applications to cryptography. Some selected topics include:

- Constructions of authentication codes from orthogonal arrays.
- Constructions of secret sharing from orthogonal arrays and cumulative arrays.
- Constructions of Group Testing from BIBDs.
- Orthogonal arrays and two-point sampling.
- Perfect hash families and broadcast encryption.