

Projects for MA 437

Here is a list of possible projects. I have scanned and posted the relevant pages and articles on <http://www4.ncsu.edu/~singer/437/437projects.html> but feel free to supplement these with other information (from the web, books, articles, ...). If you have something that interests you more than these, come and discuss it with me .

Some projects can be done by two people working together and are so designated; the others are for one person working alone. To complete a project you should read the material and write a 3-4 page summary (6-8 pages if it is two people working together) or, if it is a computer project, submit the Maple or Matlab code to me electronically. In general, I want a description of the subject with relevant definitions but no proofs. This material is due by **1 pm Wednesday, December 8.**

1. Block Designs

Project 1.1: Projective Planes This is a geometric way to construct block designs. The material is on pages 251-256 of *Introductory Combinatorics* by Kenneth Bogart.

Project 1.2: Quadratic Residues Elementary number theory can be used to produce block designs. The material is on pages 26-29 of *Applications of Abstract Algebra* by George Mackiw.

Project 1.3: Steiner Triple Systems These are block designs where each block has 3 elements. One can construct these to satisfy addition requirements, for example one can solve the following problem: You take 15 kindergarten students for a walk and arrange them in 5 rows with 3 kids in each row (so each kid has 2 companions). Can you do this for 7 days so that no two kids will be in the same row more than once? The material is in *Introductory Combinatorics* by Richard Brualdi, pages 386-393.

2. Error Correcting Codes

Project 2.1: Reed-Solomon Codes This is a project for **2 people**. The material is contained in Sections 1.7, 5.1, 5.2 of *Applications of Abstract Algebra with Maple and Matlab* by Klima, Sigmon and Stitzinger.

Project 2.2: Cyclic Codes This is a project for **2 people** unifies BCH and Hamming codes. The material is on pages 107- 119 of *Elements of Algebraic Coding Theory* by L.R.Vermani

Project 2.3: Shannon's Theorem This result examines the theoretical limits on how much

information can be transmitted through a channel. It shows that there exist very good error correcting codes but does not say how to find them (a problem that is still open). You need to be comfortable with a little probability to understand this. The material is on pages 21-30 of *Introduction to Coding Theory* by van Lint.

Project 2.3: Identification Numbers: This project is to explain how various ID numbers contain check digits that allow one to correct certain kinds of errors. You should explain the schemes contained on pages 8-14, page 23, ex, 39, 40, 41 and pages 108-110 of Gallian's book *Contemporary Abstract Algebra, Fifth Edition*.

3. Cryptography

Project 3.1: Quantum Cryptography These are crypto-systems that allow you to determine if the message has been seen by someone. The material is in a 3 page article by Erica Klarreich *Can You Keep A Secret?* and on pages 262 - 269 of *An Introduction to Cryptography* by Richard Mollin.

Project 3.2: Quadratic residues, coin-flipping by phone and zero knowledge proofs This is a project for **2 people**. Is there a way for two people at remote locations to do a coin flip fairly? Can you convince someone you have some information without revealing it? Methods to do this are described in p.401 - 411 and p.448-453 of *Elementary Number Theory and its applications* by Kenneth Rosen.

Project 3.3: Knapsack ciphers Given a set of integers a_1, \dots, a_n and an integer S , the Knapsack Problem asks if there is a subset of these integers that adds up to S . A cryptosystem based on this problem was once thought to be secure but then found to be breakable. This material is presented on p. 315-321 of *Elementary Number Theory and its applications* by Kenneth Rosen.

Project 3.4: Factoring Fermat's Little Theorem says that if p is a prime and a is a positive integer not divisible by p , then $a^{p-1} \equiv 1 \pmod{p}$. This is the basis of a method invented by Pollard in 1974 to factor integers. The material is presented on p. 215 - 220 of *Elementary Number Theory and its applications* by Kenneth Rosen. Give an exposition of this method and do problems 26 and 27 on page 221 of Rosen's book.

Project 3.5: Pseudoprimes In many cryptosystems, one needs to find prime numbers. There are some good methods that determine if a given is prime *with high probability*. These are explained on pages 223-230 of *Elementary Number Theory and its applications* by Kenneth Rosen.

Project 3.6: Vigenère Ciphers This is a project for someone who can do a little programming

in Maple or Matlab. Do exercises 3 and 5 on p. 257 of the textbook. These exercises ask one to implement the encryption, decryption and cryptanalysis of Vigenère Ciphers. You can use the canned programs given in the book and on the CD and weave them together to do this.

Project 3.7: RSA Cryptosystems This is a project for someone who can do a little programming in Maple or Matlab. Do exercises 4 and 5 on p. 289 of the textbook. These exercises ask one to implement the encryption and decryption of RSA Cryptosystems. You can use the canned programs given in the book and on the CD and weave them together to do this.

Project 3.8: Diffie-Hellman Read and summarize the 12 page article *New Directions in Cryptography* by Diffie and Hellman. The idea of a public-key cryptosystem was introduced in this paper.

Project 3.9: Public Key Crypto and Semigroups This project is rated X - it is for those who want to see current research and want a little challenge. On October 12, 2007, the paper *Public Key Cryptography based on Semigroup Actions* by Maze, Monico and Rosenthal was posted on the web (A copy can be found at the above web site). Read and summarize the first 4 pages of this article.

Project 3.10: Cayley-Purser Cryptosystem In 1999, the 16-year-old Sarah Flannery published a cryptosystem based on an unpublished work by Michael Purser, founder of Baltimore Technologies. Although the system (as a public-key crypto system) has since been found to be vulnerable to attacks, it has some interesting ideas using non-commutative groups. Flannery won several student awards for her work and, together with her mathematician father David Flannery, wrote the book *In Code: a Mathematical Journey* describing her experience. Her original paper is posted on the above website. More info can be found concerning her and the cryptosystem at wikipedia. Read and summarize Flannery's article.