Math 405, Term Projects
due Friday December 8, 2000.

Remarks: Projects can be done alone or in groups of two. Not more than two individuals/groups should choose the same project. For each project theme explain what the topic is about and what the main results are. The project is 'open ended' in the sense that you are encouraged to do computer computations when appropriate and/or provide examples and links to other research topics. The term paper you hand in should demonstrate that you mastered that topic.

1. Steiner triples and Latin squares. (See Chapter 10 of Brualdi's book).

2. Polya's counting formula. (See Chapter 14 of Brualdi's book).

3. Huffmann encoding and data compression.

4. Hamming codes and cyclic codes.

5. The MacWilliams identity.

6. Reed Solomon and BCH codes.

7. The new AES standard Rijndael. See http://csrc.nist.gov/encryption/aes/

8. Linear feedback shift registers with large period.

9. Probabilistic primality tests. (Solovay-Strassen and Miller-Rabin test).

10. The NTRU public key crypto system. See
    http://www.ntru.com/technology/tech.technical.htm

11. Elliptic curve public key systems.