MCMICHEN COLLEGE OF ARTS AND SCIENCES
Department of Mathematical Sciences

SUMMER RESEARCH OPPORTUNITIES
FOR UNDERGRADUATE WOMEN

APPLICATION DEADLINE: MARCH 1, 2005

The Department of Mathematical Sciences is pleased to offer the following research project for the summer of 2005. Interested students are urged to contact the faculty member(s) directing the project that most interests them. By contacting the faculty member, you can discover more about the project, learn what your responsibilities will be and if possible, develop a timetable for the twelve-week research period.

Implementation of Multivariable Public Key Cryptosystems

Professors Jintai Ding and Jason Gower
Arts & Sciences/Mathematical Scienecs OLD CHEM 810-A (513)556-4024 (Ding)
513 556 4937 (Gower)
FAX: (513)556-3417
E-Mail: ding@math.uc.edu; gowerj@math.uc.edu

Public key cryptosystem are encryption systems that allow us to communicate securely without any prior secret key exchange. They now play the critical role in our modern communication system such as Internet. Multivariable public key cryptosystems are new system being developed to be able to resist the future quantum computer attack and to be able to perform much more efficiently. The theoretical foundation of these systems is theory of function over finite fields. In this project, a student could work in our applied algebraic and cryptography research group at the Mathematical Sciences department in UC. The work would consists of first studying the theoretical algorithm called the perturbed Matsumoto-Imai multivariable public key cryptosystem developed by our group recently, then implementing the cryptosystem and testing its efficiency. In principle, the student would have a solid background in the basic abstract algebra theory and some significant experience with a real programming language such as Mathematica, C, or C++. In addition, a student would participate in research discussion session for our research group consisting mainly faculty and graduate students from both the mathematics department and the computer science department.