Department of Mathematical Sciences
COLLEGE OF Arts & Sciences

SUMMER RESEARCH OPPORTUNITIES
FOR UNDERGRADUATE WOMEN

APPLICATION DEADLINE: March 2, 2009

The Department of Mathematical Sciences is pleased to offer the following research project for the summer of 2009. 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.

MULTIVARIATE PUBLIC KEY CRYPTOSYSTEMS

Professor: Jintai Ding
Department of Mathematical Sciences
Office Room and Buliding: 810 Old Chemistry
Cincinnati, OH 45221-Mail Location: 0025
Tel: (513) 556-4024
Fax: (513) 556-3417
Email: jintai.ding@uc.edu

PROJECT DESCRIPTION:

Public key cryptosystems are encryption systems that allow us to communicate securely without any prior secret key exchange. They now play critical roles in our modern communication systems such as the Internet. Multivariate public key cryptosystems are new systems being developed to be able to resist future quantum computer attacks and perform much more efficiently. The theoretical foundation of these systems is the theory of functions over finite fields. In this project, a student could work in our applied algebra and cryptography research group in the Mathematical Sciences Department at UC. The work would consists of first studying the theoretical algorithm in multivariate public key cryptosystems developed by our group recently, then implementing the cryptosystem and testing its efficiency and security. I A student should have some background in basic abstract algebra theory, linear algebra and some programming experience. The student would participate in research discussion sessions for our research group consisting mainly of faculty and graduate students from both the mathematics department and the computer science department. In addition, the student can also work with other undergraduate students in a joint UC-NKU REU program supported by NSF.