Department of Mathematical Sciences
COLLEGE OF ARTS AND SCIENCES

SUMMER RESEARCH OPPORTUNITIES
FOR UNDERGRADUATE WOMEN

APPLICATION DEADLINE: March 1, 2013

The Department of Mathematical Sciences is pleased to offer the following research project for the summer of 2013. 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.

PROJECT TITLE: MULTIVARIATE and LATTICE PUBLIC KEY CRYPTOGRAPHY

Professor Jintai Ding
Department of Mathematical Sciences
4314 French Hall
Cincinnati, OH 45221-0025
Tel: (513) 556-4052
Fax: (513) 556-3417
Email: jintai.ding@gmail.com

Project Description

Public key cryptosystems are cryptosystems 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. We would not be able to online shopping without them.

Multivariate and lattice public key cryptosystems are new cryptosystems 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 and theory of lattices. In this project, a student will work in our research group in the Mathematical Sciences Department at UC. The work will consist of first studying the theoretical algorithms for multivariate and lattice public key cryptosystems, then implementing the cryptosystems and testing their efficiency and security. A student should have some background in basic abstract algebra theory and linear algebra, and some programming experiences. The student would participate in research discussion sessions of our research group and work with graduate students.