

DEPARTMENT OF MATHEMATICS COLLOQUIUM

State University of West Georgia

3:30 PM, THURSDAY, NOVEMBER 18, 2004, BOYD 301

Speaker: **Dr. Mark Faucette,**

Title: **Public Key Cryptography: The RSA Cryptosystem**

Abstract.

This talk will describe and discuss the original public key cryptosystem, the RSA algorithm. The talk will first introduce basic ideas from number theory, such as relatively prime numbers, the Euler phi function, the Euclidean algorithm, Fermat's Little Theorem, Legendre and Jacobi symbols, and primality testing. The talk will also address certain computational issues such as the repeated squaring method for computing modular arithmetic with large numbers. The RSA algorithm is then introduced and explained, including aspects of confidentiality, authenticity, non-repudiation, and integrity of data transmission. The talk is largely at an introductory level and is geared toward students. Students in number theory or in abstract algebra will find it particularly interesting.

All faculty and students are welcome.