UK MATH CLUB

Carl Cowen
Department of Mathematics
Purdue University
will speak on

"Using BIG numbers to keep BIG secrets"

Public key cryptography has been developed in the past 20 years or so and is now widely used in all kinds of security systems from encrypting data on personal computers to preserving the secrecy of military intelligence. This talk will describe the RSA cryptosystem: RSA is based on number theory, specifically, it is based on the fact that it is much more difficult to factor very large numbers than to find very large primes. The mathematics behind the RSA system will be explained and simple examples will be given. Moreover, there will be the opportunity for the audience to encrypt and decrypt messages, and perhaps even "break" an RSA code using simple mathematical software.

As always, we will have pizza and time for informal conversation with mathematics students and faculty. Carl will be happy to discuss opportunities for graduate study in Mathematics and Statistics at Purdue or elsewhere.

4 pm, Monday,
6 November 2000
Inslab, CB313

Pizza and math!

http://www.ms.uky.edu/~mathclub