CCSU

DEPARTMENT OF MATHEMATICAL SCIENCES

COLLOQUIUM

Friday, February 8
3:00 – 4:00 PM
Maria Sanford, Room 101

SOME APPLICATIONS OF FINITE GROUP THEORY

ROGER BILISOLY

CENTRAL CONNECTICUT STATE UNIVERSITY

Abstract: This talk introduces just enough group theory to look at some important applied examples. In fact, while only cyclic and permutation groups are considered, the applications include the following. First, a simple proof of the Diffie-Hellman key exchange is given followed by an example using a 100-digit prime. Second, we see how Z_{52}, the cyclic group of order 52, can model of a deck of cards using (1) the Chinese Remainder Theorem and (2) the cosets of Z_4 to represent the values ace through king and the cosets of Z_{13} for the suits. Third, we see how metric spaces can be defined on the symmetric group, S_n, and apply the L^2-norm to obtain the nonparametric correlation coefficient, Spearman's rho. Finally, we examine how Fourier transforms on cyclic groups can be used to speed up multiplication of large integers.

If you know a little about modular arithmetic and permutations, come join the fun. And if you ever wanted to know how the law of exponents can be used in the real world, this colloquium will deliver.

For further information:
gotchevi@ccsu.edu 860-832-2839
http://www.math.ccsu.edu/gotchev/colloquium/