BI-CO MATHEMATICS COLLOQUIUM

J. Robert Buchanan

Millersville University

"A Novel Geometry-Based Cryptosystem"

Monday, October 2, 2017

Talk at 4:00 – Park 338
Tea at 3:30 – Park 339, Math/Physics Lounge

Abstract:

A novel and unique cryptosystem making use of a small set of private security parameters and public initialization values to produce a pseudorandom byte stream with large period will be described. The byte stream can be used as a one-time stream cipher for securing communication between parties and for data archival. The cryptosystem makes use of geometry and number theory to generate a set of large prime integers and then from the primes a column-periodic matrix of bytes from which further calculation produces a pseudorandom, long period byte stream. The presentation discusses the design and operation of the system and states many potential questions of interest to the community of mathematical and cryptological researchers. Foremost among these questions are determining the most appropriate method for assessing the cryptographic strength of the algorithm and determining any weaknesses in the security of the algorithm.

BRYN MAWR COLLEGE