WRIGHT STATE UNIVERSITY | DEPARTMENT OF MATHEMATICS AND STATISTICS

COLLOQUIUM

Speaker: **Dr. K.T. Arasu**

Title: **Cryptography: an introduction and outline of a new cryptosystem**

Date: **Friday, September 8, 2017**

Room/Time:

Meet-n-Greet:	**2:30 p.m.**	**Room 222 MM**
Talk:	**3:00 p.m.**	**Room 224 MM**

Host: **Dr. Yuqing Chen & Dr. Qingbo Huang**

ABSTRACT:

In this day and age of the internet, transmittal of real time applications such as voice, video, images, and text across unsecured networks calls for a high level of security. Further, the advent and large-scale use of cloud storage and cloud computation systems (i.e. big data) has increased the surface area of attacks against sensitive files and information. Cryptography based encryption methods keep such sensitive information secret and secure by allowing that information to be shared securely only between authorized parties.

In this talk, we begin with the rudimentary ideas of cryptography and then present some new results that are still in preliminary stages of a manuscript: We present a new symmetric/private-key cryptosystem that we hope to provide all cyber security requirements: confidentiality, authentication and computational efficiency. Our proposed symmetric key ciphers can be composed together to produce an even a stronger cryptosystem. Our cryptosystem would use a special kind of symmetric key which has never been used before. We believe that the resulting symmetric encryption can be used: (i) In services that store encrypted data on behalf of a user (like cloud backup services, when those services leave the decryption key in the hands of the user) (ii) to encrypt computer or device storage systems (iii) to create a secure channel between two network endpoints, securely exchanging the key via public key systems, for instance. Since our proposed cryptosystem hinges on the keyspace, we develop algebraic mechanisms to construct this keyspace efficiently.

SPEAKER BIO:

K. T. Arasu has been a Professor in the Department of Mathematics and Statistics at Wright State University since 1983. He received his Master's degree in 1977 at Panjab University, India and Ph.D. in 1983 from Ohio State University. A former Humboldt fellow, he has published over 100 research articles and is on the editorial board of several prestigious journals. His research has been funded by the National Security Agency, National Science Foundation, and Air Force Office of Scientific Research. His research interests lie in the general area of applied algebra, computational methods in signal designing and signal processing and cryptography and coding theory.