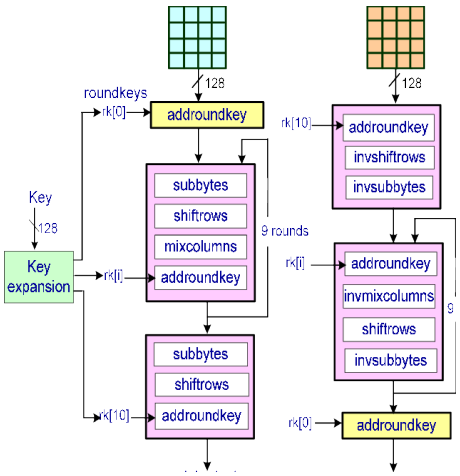
Student Research Talks (StReeTs)

Mason Experimental Geometry Lab (MEGL)

AES: The Advanced Encryption Standard

Calvin Stanley
Department of Mathematical Sciences
George Mason University



Abstract

Originally developed as the cryptosystem "Rijndael", the Advanced Encryption Standard (AES) was created by Belgian cryptographers Vincent Rijmen and Joan Daemen, and adopted by NIST in 2001. Built upon basic SPN architecture, AES is a symmetric system that has applications such as two factor authentication and government data security. In this expository talk, we examine the machinery of the algorithm, as well as various methods of its operation.on for the consistency of spectral clustering in machine learning.

Date: Friday, April 12, 2019
Time: 2:30pm–3:20pm
Place: Exploratory Hall 4106

Pizza and soda will be served at the presentation.

For further information or for special accommodations, please contact Sean Lawton via email at `slawton3@gmu.edu` or drop by the MEGL.