1089-20-244 **Kevin W Bombardier*** (kwbombardier@wichita.edu), **L. Babinkostova**, **M. Cole**, **T. Morrell** and **C. Scott**. *Algebraic Properties of Generalized Rijndael-like Ciphers.*

We provide conditions under which the set of Rijndael-like functions considered as permutations of the state space and based on operations of the finite field GF(p^k) ($p \geq 2$) is not closed under functional composition. These conditions justify using a sequential multiple encryption to strengthen the Advanced Encryption Standard (AES), a Rijndael cipher with specific block sizes. We provide conditions under which the group generated by the Rijndael-like round functions based on operations of the finite field GF(p^k) ($p \geq 2$) is equal to the symmetric group or the alternating group on the state space. (Received February 17, 2013)