1088-20-35 **Liljana Babinkostova** (liljanababinkostova@boisestate.edu), **Kevin Bombardier**, **Matthew Cole*** (mcole5@nd.edu), **Thomas Morrell** and **Cory Scott**. *AES-like ciphers over any finite field.*

We generalize the Advanced Encryption Standard (AES), which operates on the finite field $\mathrm{GF}(2^8)^{4\times 4}$, to a class of AES-like ciphers which operate on any finite field $\mathrm{GF}(p^r)^{mn}$. Sparr and Wernsdorf have explored such ciphers for $p = 2$. We determine the parity of each of the four component functions of these ciphers. We then provide conditions under which the rounds of these ciphers generate the alternating or symmetric group on the state space. Our work suggests when multiple encryption might effectively increase the security of such ciphers. (Received January 19, 2013)