1046-D1-2060 **Eric West*** (ewest@benedictine.edu), 66002. *Arithmetic in the field $F_{2^8}$ as used in the Advanced Encryption Standard.*

The Rijndael algorithm of the Advanced Encryption Standard (AES) is a symmetric-key algorithm that is in widespread use and has the official sanction of our government for all purposes. As such it seems especially pertinent to expose our students to it. However, teaching the AES to undergraduates with little advanced math background can seem a challenge, partly because of the fact that key operations of the algorithm take place in the finite field $F_{2^8}$. I will discuss the basic structure of the algorithm, how the field operations are used, and the hands-on approach I take to explain the topic in the cryptology class I have been teaching for a mixed audience of mathematics and computer science majors. (Received September 17, 2008)