1014-E1-859 **Joshua Holden*** (holden@rose-hulman.edu), Department of Mathematics, CM #125, 5500 Wabash Avenue, Terre Haute, IN 47803-3999. *Number Theory, Polynomials, and the Advanced Encryption Standard.*

While many instructors are now using cryptography to "spice up" their number theory courses, most stick either to classical ciphers like the Caesar cipher or to the RSA cryptosystem. While these are indeed good examples of the use of number theory in cryptography, instructors may not be aware that the new Advanced Encryption Standard (AES) also uses quite a bit of number theory, in the guise of finite field arithmetic, or modular arithmetic of polynomials. While the generalization from number theory to finite field arithmetic may seem a bit daunting at first, instructors and students will find that familiar concepts like the Euclidean Algorithm and modular inverses carry over quite nicely to the new setting. Furthermore, the generalization from numbers to polynomials provides an excellent "bridge" for those students who will being going on to an abstract algebra course, and an opportunity to stretch (without breaking!) the minds of those students who might not. This talk will focus on the"Simplified Advanced Encryption Standard" (S-AES) which illustrates all of the features of AES at a level of complexity which does not require the use of computers to do examples. (Received September 25, 2005)