

1046-D1-41            **Blake Rice, Neil Sigmon and Bill Yankosky\*** (byankosky@ncwc.edu), North Carolina Wesleyan College, 3400 North Wesleyan Boulevard, Rocky Mount, NC 27894. *The ElGamal Cryptosystem on the TI-83*. Preliminary report.

Like the RSA cryptosystem, implementation of the ElGamal cryptosystem over the group of units modulo  $p$ , where  $p$  is a prime, is relatively simple in that it only requires students to have an understanding of exponentiation, modular arithmetic and some elementary group theory properties. All of these topics are accessible to students, even those who are not necessarily majoring in mathematics. Using a TI-83 to aid in the implementation of cryptosystems allows students to be able work with larger integers than they could feasibly work with by hand. The purpose of this presentation is to show how some graphing calculator programs can be used to implement the basic ElGamal cryptosystem over the group of units modulo  $p$  using the TI-83. (Received June 28, 2008)