

1077-VJ-2131      **Lavinia Ciungu\*** (LCiungu@uco.edu), 100 N University Drive, Edmond, OK 73034, and **Mark Wissler**. *Encrypting into Polynomials*. Preliminary report.

In cryptography, two well-known problems are the RSA algorithm, whose core difficulty resides in factorizing a large integer into a product of primes, and the ElGamal algorithm, which is based off of the difficulty that arises while trying to solve the discrete log problem. In the vein of the Jacobian conjecture, this study examines the cryptographic implications of encrypting messages into polynomials based off of a function,  $F(x, y)$ , whose inverse exists. Utilizing this function, each element of a message is placed into a polynomial mapping family and evaluated by  $F$ . Each element is then evaluated and output into a polynomial. Using this method, the encryption of messages is a fairly easy process, while the decryption requires finding the inverse of the decryption function, which is a difficult task. (Received September 21, 2011)