The ElGamal Public-Key Cryptosystem – A Full Implementation Using DERIVE

J.Wiesenbauer

Department of Discrete Mathematics
Vienna University of Technology
Austria

j.wiesenbauer@tuwien.ac.at

Lecture Proposal for the TI-Nspire & Derive Strand

ABSTRACT

The ElGamal cryptographic scheme is along with RSA one of the most widely used public-key cryptosystems, in particular when it comes to the use on smartcards and small devices due to its relatively small need of resources in some variants. From a mathematical point of view, the underlying “hard” mathematical problem is the discrete logarithm problem (DLP). While it can be formulated for any group, usually the multiplicative group of a finite field or groups emerging from elliptic curves are used in this context.

In my talk using DERIVE a full implementation of the ElGamal cryptosystem is provided using elliptic curves over finite residue class rings mod p, where p is a prime with at least 160 bits, including the signature scheme as proposed by NIST. As for the problem of determining the order of the involved elliptic curves we make use of so-called CM-curves for this purpose. Furthermore the most common attacks on DLP like Baby-step-giant-step algorithm, Pollard’s rho-method and the Pohlig-Hellman method are discussed, along with implementations and a lot of examples.

Keywords

ElGamal cryptosystem, Public-key cryptosystems, discrete logarithm problem, elliptic curves