CORR 2002-01

Generating Large Instances of the Gong-Harn Cryptosystem

Kenneth J. Giuliani, Guang Gong*

Abstract In 1999, Gong and Harn proposed a new cryptosystem based on third-order characteristic sequences over finite fields. This paper gives an efficient method to generate instances of this cryptosystem over larege finite fields. The method first finds a "good" prime p to work with and then constructs the sequence to ensure that it has the desired period. This method has been implemented in C++ using NTL[7] and so timing results are presented.