

1067-C5-706

Daniel Cabarcas* (cabarcd@mail.uc.edu). *Algebraic Cryptanalysis as a tool for teaching Cryptology.*

This work originates from the experience of three summer REUs in mathematical cryptology organized jointly by Chris Christensen (Northern Kentucky University) and Jintai Ding (University of Cincinnati) between 2008 and 2010. The central theme of the program was algebraic cryptanalysis, that is, breaking cryptosystems by solving systems of polynomial equations. We will summarize the experience highlighting the role played by algebraic cryptanalysis as a pedagogical tool for teaching cryptology. (Received September 13, 2010)