1046-68-735 **Delaram Kahrobaei*** (dkahrobaei@gc.cuny.edu), Doctoral Program in Computer Science, CUNY Graduate Center, 365 Fifth Avenue, New York, NY 10016, and **Michael Anshel** (csmma@cs.ccny.cuny.edu), Department of Computer Science, City College of New York, 138th Street & Convent Ave, New York, NY 10031. *A Gateway to Group based Cryptography.* Preliminary report.

Group-based cryptography has emerged as an exciting interdisciplinary area (see [MSV]). Our purpose is to show polycyclic groups(see [S], [HEO], [EK], [KK]) offer a gateway to group based cryptography. We show how classical public-key algorithms can naturally be formulated with in the context of polycyclic groups, and test it, using the framework of group based cryptography.

[MSU] Myasnikov, Shpilrain, Ushakov, Group-based cryptography, Birkhauser, 2008.

[S]Segal, Polycyclic groups. Cambridge Tracts in Mathematics, 82. Cambridge University Press, Cambridge, 1983

[HEO]Holt, Eick, O'Brien, Handbook of computational group theory. Chapman & Hall, 2005

[EK] Eick, Kahrobaei, Polycyclic Groups: New Platform for Cryptology? 2004

[KK]Kahrobaei, Khan: Non-commutative Generalizations of El Gamal using Polycyclic Groups, Proceeding of IEEE, 2006 (Received September 10, 2008)