1060-20-131

David Garber* (garber@hit.ac.il), Holon Institute of Technology, 52 Golomb St., PO Box 305, 58102 Holon, Israel. *Length-based attack on a cryptosystem based on polycyclic groups.* Preliminary report.

In many situations, we need to transfer data in a secure way: credit cards information, health data, security uses, etc. The idea of public key cryptography in general is to make it possible for two parties to agree on a shared secret key, which they can use to transfer data in a secure way.

Combinatorial group theory is a fertile ground for finding hard problems which can serve as a base for a cryptosystem. Eick and Kahrobaei (2004) have suggested a possible cryptosystem based on polycyclic groups.

In the talk, we will present the cryptosystem, our implementation of the length-based attack for this case, and some preliminary results. Joint work with Assaf Balleli. (Received March 27, 2010)