1046-20-1948 **Alexei Miasnikov*** (alexeim@math.mcgill.ca), Department of Mathematics and Statistics, 805 Sherbrooke St. West, Montreal, Quebec H3A 2K6, Canada. *Mathematics of Commutator Key Exchange.* Preliminary report.

This talk is about some recent developments in non-commutative cryptography. The main focus will be on mathematical problems that arise here, and how solutions to these problems may affect security of various public key exchange schemes. I will discuss on how the classical algebraic algorithmic problems may be used in cryptography, and what should be avoided; why undecidable decision problems may play a part in cryptanalysis of real cryptosystems, and what kind of practical knowledge one can get from asymptotic methods. Most of the ideas that occur here are quite general, but I will try to explain them on one particular example - the commutator key exchange schemes based on groups. The talk is based on joint work with R.Gilman, A.Myasnikov, and A.Ushakov. (Received September 16, 2008)