ABSTRACT

The thesis is presented in 46 pages. It contains 2 appendixes and bibliography of 6 references. Eight figures and one table are given in the thesis.

The goal of the thesis is to develop mathematical and software tools for asymmetric system of enciphering Merkela-Hellmana and research of using LLL-algorithm for its cryptoanalysis.

System of enciphering which was built on a NP-full task of laying of a backpack is considered. The way of cryptoanalysis for this system with LLL- algorithm for build short basis integral lattices is discussed.

The automated system for enciphering and enciphering are developed, also cryptoanalysis for its is developed too. The developed system is tested.

Keywords: asymmetric system of enciphering, task of laying of a backpack, modular multiplication, LLL- algorithm for build short basis integral lattices.