ANNOTATION

Diploma project title: " Software system of cryptanalysis using impossible differentials method based on parallel programming technologies OpenMP and MPI".

Objective is to design sequential and parallel algorithms for the analysis of the stability of block ciphers using impossible differentials and identify the implementation details of its main stages.

The subject of the study. The subject of research is the use of differential cryptanalysis features and method of impossible differentials in evaluating sustainability of block ciphers.

The object of study . Object is a block encryption algorithm AES, in particular, the elements that make up round algorithm.

The program is being developed in this project is designed for cryptanalysis using impossible differentials method of symmetric block cipher AES, namely - the elements round

Explanatory memorandum consists of six chapters.

The first section is the staging . Here is a brief overview of current methods of cryptanalysis , a theoretical analysis of the subject , defines the goals and objectives of the project work master , and basic solutions. In addition, the first chapter deals with the analysis of block ciphers and scope of AES, the relevance of cryptanalysis , as such , methods of cryptanalysis , exhaustive search method , the birthday paradox , parallelism in problems of cryptanalysis , the conclusions formulated by the choice of methods that are best suited for creating a software system .

The second section is devoted to algorithms that are used in the work. These include a full review of the encryption algorithm AES (Rijndael), including rounder conversion algorithm key generation , encryption , decryption function return , the direct decoding . In addition, the second section describes the methods of cryptanalysis , namely the differential cryptanalysis and MND . Recently viewed under use MPI for

parallelization cryptanalysis . Conclusions to the second section summarizes the choices of the algorithm, and shows the main characteristics of methods or algorithms.

The third part involves writing software. It describes the main elements of the AES, and conduct cryptanalysis MND over them. Also considered parallelization of source code using MPI, and written testing software.

The fourth chapter - economic. The main purpose of the section is to establish the feasibility of conducting development.

Fifth chapter - part of occupational health and safety. It deals with security when working with computers, and security in emergency situations.

The sixth section - Section of Ecology.

Release year - 2013 .

Year of protection - 2013 .

Keywords : impossible differentials method, cryptanalysis , AES.

Thesis contains 143 pages, 14 tables, 23 figures, 22 references.