БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе

АНАЛИЗ И РЕАЛИЗАЦИЯ КРИПТОСИСТЕМЫ BELT

Петроченко Виктория Андреевна

Научный руководитель:
кандидат физ.-мат. наук,
доцент Д. Н. Чергинец

2020

В дипломной работе 150 страниц, 22 рисунка, 15 таблиц, 5 источников, 12 приложений.

Ключевые слова: ШИФРОВАНИЕ ИНФОРМАЦИИ, ПОТОЧНОЕ ШИФРОВАНИЕ, БЛОЧНОЕ ШИФРОВАНИЕ, КРИПТОГРАФИЧЕСКИЙ АЛГОРИТМ, КРИПТОСИСТЕМА BELT, ДИНАМИЧЕСКАЯ БИБЛИОТЕКА КЛАССОВ, ЯЗЫК ПРОГРАММИРОВАНИЯ C#.

В дипломной работе изучаются общий принцип работы поточного и блочного шифрования, режимы работы блочного шифрования, особенности работы алгоритмов криптосистемы BelT.

Целью дипломной работы является анализ работы режимов блочного шифрования, анализ работы алгоритмов криптосистемы BelT и програмная реализация криптосистемы BelT.

В дипломной работе получены следующие результаты:

1. Описан общий принцип функционирования поточных и блочных криптосистем;
2. Описаны и сопоставлены режимы функционирования блочных криптосистем;
3. Подробно описана работа алгоритмов криптосистемы BelT;
4. Разработана и верифицирована динамическая библиотека классов на языке программирования C#, реализующая алгоритмы криптосистемы BelT.

Дипломная работа носит теоретический (практический) характер. Ее результаты могут быть использованы при изучении шифрования информации, а разработанная библиотека классов может быть использована для обеспечения безопасности данных.

Достоверность полученной библиотеки классов обусловлена ее верификацией на тестовых наборах, предоставленных стандартом криптосистемы BelT.

Дипломная работа выполнена автором самостоятельно.

Thesis project is presented in the form of an explanatory note of 150 pages, 22 figures, 15 tables, 5 references, 12 applications.

ENCRYPTION INFORMATION, STREAM ENCRYPTION, BLOCK ENCRYPTION, CRYPTOGRAPHIC ALGORITHM, CRYPTOSYSTEM BELT, DYNAMIC CLASSES LIBRARY, PROGRAMMING LANGUAGE C#.

The research object is to study the general principle of the work of stream and block encryption, the modes of operation of block encryption, the features of the

cryptosystem BelT.

The purpose of the thesis is to analyze the operation of block encryption modes, analysis of the operation of BelT cryptosystem algorithms and software implementation of the BelT cryptosystem.

The main results of the thesis projects are as follows:

1. The general principle of the operation of stream and block cryptosystems is described;

2. The operation modes of block cryptosystems are described and compared;

3. The operation of BelT cryptosystems algorithms is described in detail;

4. A dynamic class library in the C# programming language was developed and verified that implements BelT cryptosystem algorithms.

This thesis project is a theoretical/practical one. Its results can be used in the study of information encryption, and the developed class library can be used to ensure data security.

The reliability of the resulting class library is due to its verification on test suites provided by the BelT cryptosystem standard.

The thesis project was done solely by the author.