МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

«Вероятностно-статистический анализ криптографического преобразования Фейстеля»

Кивель Ольга Сергеевна

Научный руководитель - доктор физ.-мат. наук, профессор,
чл.-корр. НАН Беларуси Ю.С. Харин

Минск, 2020

РЕФЕРАТ

Дипломная работа: 67 страниц, 31 рисунок, 22 таблицы, 36 источников, 1 приложение.

Ключевые слова: КРИПТОСИСТЕМА, КРИПТОГРАФИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ, КРИПТОГРАФИЧЕСКОЕ ИТЕРАЦИОННОЕ ПРЕОБРАЗОВАНИЕ ФЕЙСТЕЛЯ.

Цель исследования: провести вероятностно-статистический анализ криптографического преобразования Фейстеля.

Объект исследования: стойкость криптографического преобразования Фейстеля.

Методы исследования: теоретические, общелогические, эмпирические методы, методы криптографии, методы теории вероятностей и математической статистики.

Результат работы: определены показатели стойкости преобразования Фейстеля, разработана программа для получения численных оценок стойкости, проведены компьютерные эксперименты по анализу показателей стойкости преобразования Фейстеля.

Область применения: криптографические системы на основе преобразования Фейстеля.

ABSTRACT

Diploma thesis: 67 pages, 31 figures, 22 tables, 36 sources, 1 attachment.

Key words: CRYPTOSYSTEM, CRYPTOGRAPHIC TRANSFORMATION, THE ITERATIVE CRYPTOGRAPHIC TRANSFORMATION OF FEISTEL.

Work purpose: perform a probabilistic and statistical analysis of the Feistel cryptographic transformation.

Object of research: stability of the Feistel cryptographic transformation.

Research methods: theoretical, general logical, empirical methods, methods of cryptography, methods of probability theory and mathematical statistics.

Results: the Feistel transformation stability indicators were determined, a program was developed to obtain numerical stability estimates, and computer experiments were conducted to analyze the Feistel transformation stability indicators.

Application area: cryptographic systems based on the Feistel transform.