МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

“Построение “сильных” S-блоков упрощённого шифра ГОСТ на основе максимизации характеристики перемешивания”

Доросев Евгений Алексеевич

Научный руководитель – кандидат физико-математических наук, доцент кафедры математического моделирования и анализа данных Волошко В. А.

Минск, 2024

РЕФЕРАТ

Дипломная работа: 54 страницы, 2 главы, 19 рисунков, 6 таблиц, 14 использованных источников, 1 приложение.

Ключевые слова: БЛОЧНАЯ КРИПТОСИСТЕМА, S-БЛОК, ГОСТ 28147-89, ЦЕПЬ МАРКОВА, ДЕРЕВО, СОБСТВЕННЫЕ ЗНАЧЕНИЯ.

Объект исследования: S-блоки, их применения в блочных шифрах в качестве элемента рассеивания и перемешивания.

Цель работы: анализ скорости перемешивания, её зависимость от второго абсолютного собственного значения матрицы переходных вероятностей. Построение семейства упрощённых шифров ГОСТ 28147-89 и нахождение на нём наилучшего семейства S-блоков при выбираемых параметрах.

Методы исследования: а) теоретические: изучение источников, посвящённых блочным криптосистемам и используемых в них S-блоках, применяемым для шифрования информации; изучение методов анализа и характеристик этих блоков;

б) практические: разработка программной реализации упрощённого шифра ГОСТ 28147-89, а также выбранных методов анализа.

Результат: сравнение типов S-блоков и описание их влияния на перемешивание и рассеивание, связь с выбранной характеристикой перемешивания; реализация на языке программирования Python семейства упрощённого шифра ГОСТ 28147-89 и методов анализа S-блоков.

Область применения: криптографическая сфера.

ABSTRACT

Diploma thesis: 54 pages, 2 chapters, 19 figures, 6 tables, 14 sources, 1 attachments.

Keywords: BLOCK CRYPTOSYSTEM, S-BLOCK, GOST 28147-89, MARKOV CHAIN, TREE, EIGENVALUES.

Object of study: S-boxes, their applications in block ciphers as a scattering and mixing element.

Purpose of work: analysis of the mixing rate, its dependence on the second absolute eigenvalue of the transition probability matrix. Construction of a family of simplified GOST 28147-89 ciphers and finding the best family of S-boxes on it with selected parameters.

Research methods: a) theoretical: study of sources devoted to block cryptosystems and the S-blocks used in them, used to encrypt information; studying methods of analysis and characteristics of these blocks;

b) practical: development of a software implementation of a simplified GOST 28147-89 cipher, as well as selected analysis methods.

Result: comparison of S-box types and description of their influence on mixing and dispersion, connection with the selected mixing characteristic; implementation in the Python programming language of the simplified GOST 28147-89 cipher family and S-box analysis methods.

Scope: the cryptographic field.