МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

“Автоматические средства оценки надёжности блочных криптосистем”

Свирид Полина Дмитриевна

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

Минск, 2024

РЕФЕРАТ

Дипломная работа**:** 53 с., 2 рис., 2 табл., 12 листингов, 24 источника, 2 прил.

Ключевые слова: БЕЗОПАСНОСТЬ, БЛОЧНАЯ КРИПТОСИСТЕМА, АТАКА РАСПОЗНАВАНИЯ, ХАРАКТЕРИСТИКА.

Объект исследования: объектом исследования являются блочные криптосистемы, в частности государственный стандарт симметричного шифрования Республики Беларусь Belt.

Цель исследования: рассмотреть автоматические средства оценки надёжности блочных криптосистем. Оценить надёжность государственного стандарта симметричного шифрования Республики Беларусь Belt.

Методы исследования: а) теоретические: изучение литературы, посвящённой описанию атак распознавания на блочные криптосистемы, автоматизированным средствам для оценки надёжности блочных криптосистем и методам, лежащим в основе данных автоматизированных средств. б) практические: используя автоматизированный инструмент CASCADA, оценить надёжность государственного стандарта симметричного шифрования Республики Беларусь Belt.

Полученные результаты: получены оценки надёжности государственного стандарта симметричного шифрования Республики Беларусь Belt с помощью средства CASCADA, которое ранее не применялось для оценки надежности Belt.

Область возможного применения: теоретическая и практическая криптография.

ABSTRACT

Degree paper**:** 53 p., 2 ill., 2 tab., 12 listings, 24 sources, 2 app.

Key words: SECURITY, BLOCK CRYPTOSYSTEM, DISTINGUISHING ATTACK, CHARACTERISTIC.

Object of research: the object of the research is block ciphers, in particular Belt — the state standard of symmetric encryption of the Republic of Belarus.

Purpose of research: is to consider the automatic tools used to evaluate the security of block ciphers. To evaluate the security of the state standard of symmetric encryption of the Republic of Belarus (Belt).

Research methods: are a) theoretical: the study of the literature devoted to the description of distinguishing attacks on block ciphers, automatic tools for evaluating the security of block ciphers and the methods underlying these automatic tools. b) practical: using the automatic tool CASCADA, evaluate the security of the state standard of symmetric encryption of the Republic of Belarus (Belt).

Obtained results and their novelty: security estimates of the state standard of symmetric encryption of the Republic of Belarus (Belt) were obtained using the tool CASCADA. CASCADA hasn’t previously been used to evaluate the security of the Belt.

Area of possible application: is theoretical and practical cryptography.