МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе

АНАЛИЗ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ МЕСЕНДЖЕРА TELEGRAM

Игнатюк Иван Сергеевич

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

2021

В данной дипломной работе 55 страниц, 5 таблиц и 4 рисунка.

TELEGRAM, СЕКРЕТНЫЕ ЧАТЫ, ШИФРОВАНИЕ TELEGRAM, АЛГОРИТМ AES IGE, ПРОТОКОЛЫ ШИФРОВАНИЯ TELEGRAM.

Объектом исследования является мессенджер Telegram.

Целью данной работы является изучение и криптоанализ протоколов передачи данных Telegram. Устойчивость протокола к атакам человек посередине и атаки с помощью открытых текстов. Реализация алгоритма создания ключа авторизации пользователя.

Теоретическую основу дипломной работы в основном составляет документация Telegram и зарубежные статьи.

В дипломной работе были получены следующие результаты:

1. Изучены протоколы передачи данных Telegram.
2. Изучены шифрование и дешифрование данных в Telegram.
3. Проведен анализ передачи данных в секретных и обычных чатах.
4. Реализован алгоритм генерации ключа авторизации.
5. Получены теоретические выводы и практические рекомендации.

Дипломная работа является теоретически-практической. Ее результаты могут быть использованы в улучшении защиты криптографичских протоколов Telegram и понимания их работы.

Дипломная работа является завершенной, поставленные задачи выполнены в полной мере, присутствует возможность дальнейшего развития работы.

Дипломная работа выполнена автором самостоятельно.

Thesis project is presented in the form of an explanatory note of 55 pages, 5 tables and 4 figures.

TELEGRAM, SECRET CHATS, TELEGRAM ENCRYPTION, AES IGE ALGORITHM, TELEGRAM ENCRYPTION PROTOCOLS.

The research object of this thesis project is to study protocols of messenger Telegram.

The purpose of this work is study and analysis of Telegram’s data transfer protocols. The protocol's resilience to man-in-the-middle attacks and open-text attacks. Implementation of the algorithm for creating a user authorization key.

The theoretical basis of the thesis is mainly made up of Telegram documentation and foreign articles.

The main results of the thesis project are as follows:

1. The Telegram data transfer protocols was described.

2. We described how data in Telegram is encrypted and decrypted.

3. The analysis of data transmission in secret chats and regular chats was carried out.

4. The algorithm for generating the authorization key was constructed.

5. Theoretical conclusions and practical recommendations were obtained.

The thesis is theoretical and practical. Its results can be used to improve the security of Telegram's cryptographic protocols and to understand how they work.

The thesis is completed, the tasks are completed in full, there is the possibility of further development of the work.

The thesis was completed by the author independently.