АНОТАЦІЯ

Добровольський А.О. “Дослідження та покращення алгоритмів блочного шифрування даних” – Рукопис.

Мета дослідження полягає у вивченні роботи алгоритму блокового шифрування даних DES з метою його модифікації для збільшення криптостійкості, а також створення застосунку, який демонструє шифрування та розшифрування даних за допомогою модифікованого алгоритму.

Досліджено сучасні підходи до шифрування та розшифрування даних. Досліджено основні симетричні алгоритми блочного шифрування даних. Проаналізовані сильні й слабкі сторони симетричного алгоритму DES.. Розроблено архітектуру застосунку. Програмно реалізовано алгоритм DES та його модифікації.

Створений програмний засіб дає змогу виконати швидке шифрування великої кількості даних для наступної передачі їх по відкритому каналу отримувачеві без попередньої передачі ключа.

Отриманні результати можуть бути використанні будь-якими користувачами, які хочуть безпечно обмінюватись інформацією.

Ключові слова: ШИФРУВАННЯ, КРИПТОГРАФІЧНА СТІЙКІСТЬ, СИМЕТРИЧНІ КРИПТОСИСТЕМИ, СИСТЕМИ ГЕНЕРАЦІЇ КЛЮЧІВ, АУТЕНТИФІКАЦІЯ КРИПТОГРАФІЧНИЙ КЛЮЧ, РАНДОМІЗАЦІЯ, ЦИКЛ ФЕЙСТЕЛЯ, БЛОКОВИЙ ШИФР .NET CORE, C#.

SUMMARY

Dobrovolsky A.O. "Research and improvement of existing block encryption algorithms" - Manuscript.

The aim of the research is to study the operation of the algorithm of block data encryption DES with the purpose of modifying it to increase the cryptographic strength, and also to create an application demonstrating the encryption and decryption of data using a modified algorithm.

The modern approaches to encryption and decryption of data are explored. The main symmetric algorithms of block data encryption are investigated. The strengths and weaknesses of the symmetric DES algorithm are analyzed. The architecture of the application is developed. The DES algorithm and its modifications are implemented programmatically.

The created software allows to perform fast encryption of a large amount of data for subsequent transfer through the open channel to the recipient without preliminary transfer of the key.

The results obtained can be used by any users who want to exchange information securely.

Keywords: ENCRYPTION, CRYPTOGRAPHIC RESISTANCE, SYMMETRIC CRYPTO SYSTEMS, KEY GENERATION SYSTEMS, AUTHENTICATION OF THE KRIPTOGRAPHIC KEY, RANDOMIZATION, FEISTLE CYCLE, BLOCK CODE. NET CORE, C #.

АННОТАЦИЯ

Добровольский А.О. "Исследование и улучшение алгоритмов блочного шифрования данных" - Рукопись.

Цель исследования заключается в изучении работы алгоритма блочного шифрования данных DES с целью его модификации для увеличения криптостойкости, а также создание приложения, демонстрирующего шифрование и расшифровку данных с помощью модифицированного алгоритма.

Исследованы современные подходы к шифрованию и расшифровке данных. Исследованы основные симметричные алгоритмы блочного шифрования данных. Проанализированы сильные и слабые стороны симметричного алгоритма DES. Разработана архитектура приложения. Программно реализован алгоритм DES и его модификации.

Созданное программное средство позволяет выполнить быстрое шифрование большого количества данных для последующей передачи их по открытому каналу получателю без предварительной передачи ключа.

Полученные результаты могут быть использованы любыми пользователями, которые хотят безопасно обмениваться информацией.

Ключевые слова: ШИФРОВАНИЕ, КРИПТОГРАФИЧЕСКАЯ СТОЙКОСТЬ, СИММЕТРИЧНЫЕ КРИПТОСИСТЕМИ, СИСТЕМЫ ГЕНЕРАЦИИ КЛЮЧЕЙ, АУТЕНТИФИКАЦИЯ КРИПТОГРАФИЧЕСКОГО КЛЮЧА, РАНДОМИЗАЦИЯ, ЦИКЛ ФЕЙСТЕЛЯ, БЛОЧНЫЙ ШИФР .NET CORE, C #.