БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра многопроцессорных систем и сетей

Аннотация к дипломной работе

“Сервис декодирования файлов”

Макарушко Ирина Александровна

Научный руководитель – ст. преподаватель Сакович В.Ю.

2016

Реферат

Дипломная работа, 49 страниц, 19 рисунков, 1 таблица, 9 источников.

АТАКА, МОНОАЛФАВИТНЫЙ ШИФР, МНОГОАЛФАВИТНЫЙ ШИФР, РАСШИФРОВКА, АЛГОРИТМ, СТАТИСТИКА, ГЕНЕТИЧЕСКИЙ АЛГОРИТМ, RSA, РЕФЛЕКСИЯ, МНОГОЯЗЫКОВАЯ ПОДДЕРЖКА, MVC, SPRING.

Объект исследования – алгоритмы расшифровки текстов.

Цель исследования – изучить подходы криптоанализа шифров, разработать легко расширяемую систему декодирования файлов.

За время работы были реализованы следующие задачи: реализованы алгоритмы дешифровки RSA, блочного перестановочного шифра, шифра Плейфера, шифра Виженера, шифра Цезаря; разработана легко расширяемая система декодирования файлов; добавлена поддержка двух языков: русского и английского.

В работе рассматривалась атака только на зашифрованные тексты, то есть на вход система получала текстовый файл без каких-либо сведений об алгоритме шифрования. Для криптоанализа использовались статистические методы, метод грубой силы и генетический алгоритм.

Область применения – сервисы, которые специализируются на расшифровке файлов.

Abstract

Diploma thesis, 49 pages, 19 figures, 1 table, 9 sources.

ATTACK, MONO-ALPHABETIC CIPHER, MULTIPLE-ALPHABET CIPHER, DECIPHERING, ALGORITHM, STATISTICS, GENETIC ALGORITHM, RSA, REFLEXION, MIXED-LANGUAGE SUPPORT, MVC, SPRING.

Object of research – decryption algorithms for texts.

Purpose – to explore cryptanalysis techniques, to develop easily expandable system for decryption of files.

During the work completed the following tasks: decryption algorithms were realized for RSA, block permutation cipher, Vigenere cipher, Playfair cipher, Caesar cipher; easily expandable system for decryption of files was implemented; it was added support for the Russian language and the English language.

The diploma thesis covered a ciphertext-only attack, the system takes input a txt file without any information about algorithm of encryption. It was used statistical methods, brute force method and genetic algorithm for cryptanalysis.

Application field – services that specialize in decryption of files.