

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра системного анализа и компьютерного моделирования

ЧЭНЬ ЦЗЯХАО

**РАЗРАБОТКА НА ПЛАТФОРМЕ RASPBERRY ПО
ДЛЯ КРИПТОАНАЛИЗА ПОЛИАЛФАВИТНЫХ ШИФРОВ**

Аннотация (реферат) дипломной работы

Научный руководитель:
старший преподаватель,
П.П. Коржуков

Допущена к защите
«__» _____ 2024 г.
Зав. кафедрой системного анализа
и компьютерного моделирования
канд. физ.-мат. наук, доцент

Н.Н. Яцков

Минск, 2024

РЕФЕРАТ

Дипломная работа содержит 62 страницы, 12 иллюстраций, 18 источников, 2 приложения.

Ключевые слова: БИБЛИОТЕКА ФУНКЦИЙ C/C++, ВЗАИМНАЯ КОРРЕЛЯЦИОННАЯ ФУНКЦИЯ, ГИСТОГРАММА ЧАСТОТ, ИНТЕГРИРОВАННАЯ СРЕДА РАЗРАБОТКИ, ИНДЕКС СОВПАДЕНИЙ, КРИПТОАНАЛИЗ, МЕТОД КАСИСКИ, МЕТОД ФРИДМАНА, МИКРОКОМПЬЮТЕР, ОПЕРАЦИОННАЯ СИСТЕМА, ПОЛИАЛФАВИТНЫЙ ШИФР, ПРОГРАММА, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ШИФР, ШИФР ВИЖЕНЕРА, ШИФР ЗАМЕНЫ, ARM, RASPBERRY PI.

Объект исследования – криптоанализ полиалфавитных шифров с алфавитами на кириллице, проводимый с помощью микрокомпьютера.

Предмет исследования – программное обеспечение инструментария для криптоанализа полиалфавитных шифров с привлечением микрокомпьютера Raspberry Pi.

Цель работы – исследовать работу с микропроцессорами на основе архитектуры ARM, в частности с микрокомпьютерами семейства Raspberry Pi, на примере разработки программного инструментария для криптоанализа полиалфавитных шифров.

Разработка программной системы инструментария криптоанализа выполнена с использованием набора инструментов (toolchain) ИСР Geany.

ABSTRACT

本论文共 62 页，12 幅插图，18 个资料来源，2 个附录。

关键词：C/C++函数库、互相关函数、频率直方图、集成开发环境、重合指数、密码分析、卡西斯基法、弗里德曼法、微型计算机、操作系统、多字母密码、程序、软件、密码、类型密码，替换密码、ARM、树莓派。

该研究的目的：使用微型计算机对带有西里尔字母的多表密码进行密码分析。

该研究的主题：使用 Raspberry Pi 微型计算机对多表密码进行密码分析的软件工具。

这项工作的目的：探索使用基于 ARM 架构的微处理器，特别是使用 Raspberry Pi 系列的微型计算机，以开发用于多表密码密码分析的软件工具为例。

密码分析工具软件系统的开发是使用 IDE 工具链进行的。Geany