Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Владимирский государственный университет

имени Александра Григорьевича и Николая Григорьевича Столетовых»

(ВлГУ)

Кафедра Информатики и защиты информации

Лабораторная работа

На тему Средство криптографической защиты информации”

Выполнил:

Студент группы ИCБ-118

Катков А.Н.

Принял:

Монахов Ю.М.

Владимир 2021

**Задание:**

Реализация криптографической системы защиты информации должна выполнять:

* Генерацию ключа
* Шифрование и дешифрование файла на ключе
* Шифрование и дешифрование папки на ключе

В ходе выполнения лабораторной работы было разработано приложение под ОС Windows:

* с дружественным и понятным интерфейсом
* с наличием справки по основным аспектам программы

В результате выполнения лабораторных работ было реализовано клиент серверное приложение СКЗИ. Для шифрования данных приложение использует реализацию алгоритма CAST-128.

CAST-128 – это блочный алгоритм симметричного шифрования на основе сети Фейстеля. Размер ключа 40, 48, 56, 64, ..., 112, 120, 128 бит. Размер шифруемого алгоритмом блока 64 бит, число раундов составляет 12, однако при длине ключа больше 80 бит количество раундов увеличивается до 16. Полное описание алгоритма приведено в документе RFC 2144.

Алгоритм был доработан, тем что использует режим сцепления блоков шифротекста (CBC) Для генерации ключа программа генерирует ключ для AES, а затем обрезает его до размера ключа необходимого используемому алгоритму, в программе при выборе размера ключа, го размер приведен в байтах.

В качестве клиентской часты выступает программа предоставляющая интерфейс и возможности для регистрации/авторизации, шифрования/дешифрования. Клиент написан на языке python. Запускается без интерпретатора.

На сервере содержатся следующие таблицы:

* первая с логином и паролем
* вторая с содержит логин, хэш хэша первых 64000 бит шифрованного файла, два сгенерированных ключа, вектор инициализации, размер остатка блока и длину изначального ключа.

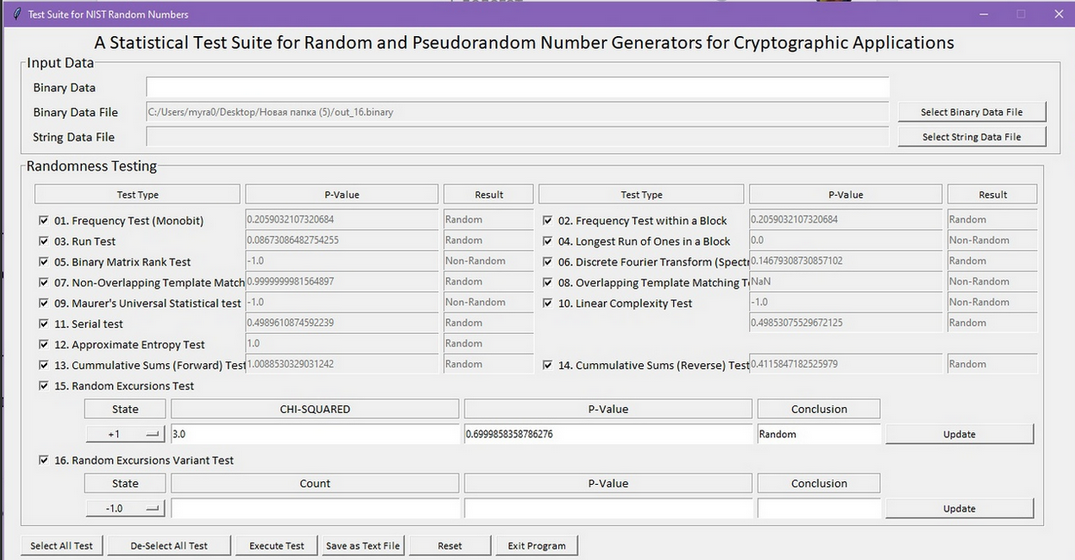
Сервер при запуске не нуждается в предустановленной jre/jdk/

В БД(database.db) данные хранятся в зашифрованном на логине пользователя виде (логин еще и захэширован) по алгоритму aes-256 ECB.

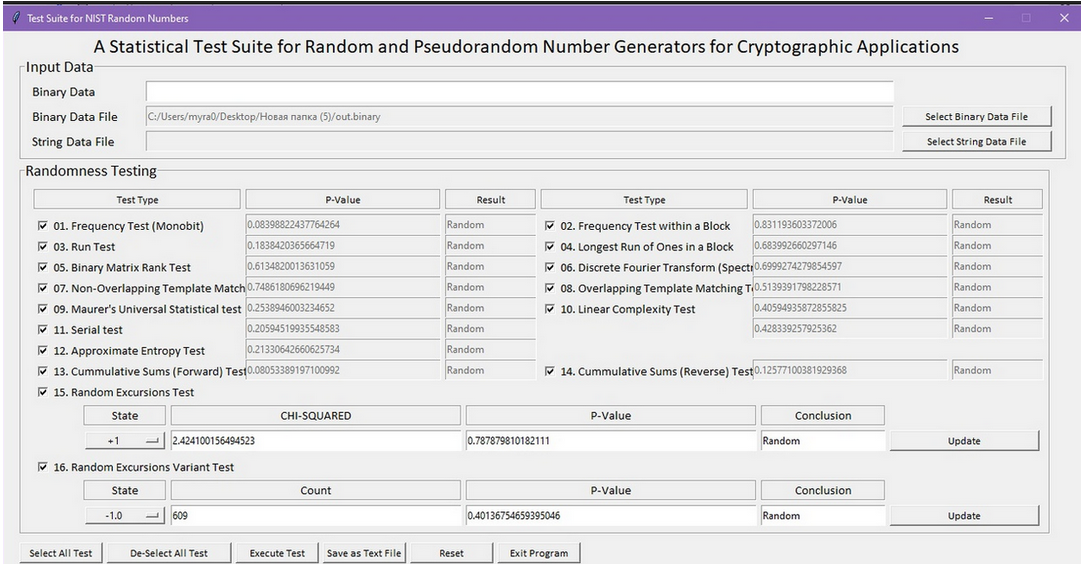
Также для шифрования папки и файлы не должны содержать в своих названиях пробелы. В результате работы программа выводит сообщение со временем затраченным на шифрование/дешифрование, с учетом времени на архивацию.

Результаты проведенного NIST тестирования:

Ключ



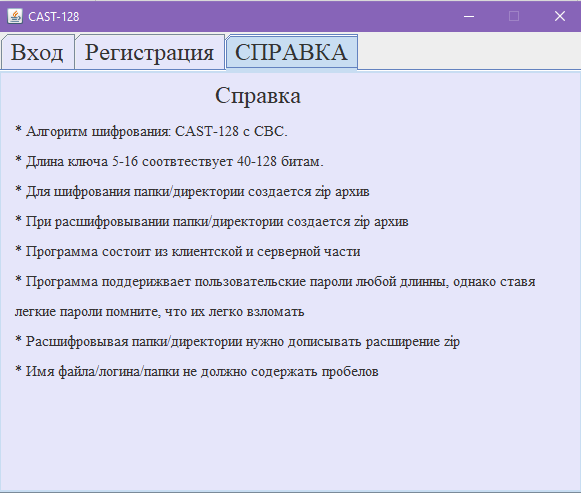
Зашифрованный файл



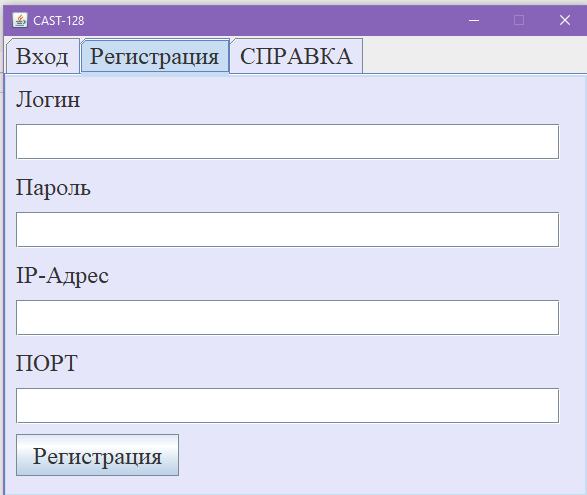
Видео работы программы доступно в репозитории по ссылке (https://github.com/Physalis-1/kripta)

**Примеры реализованной программы**

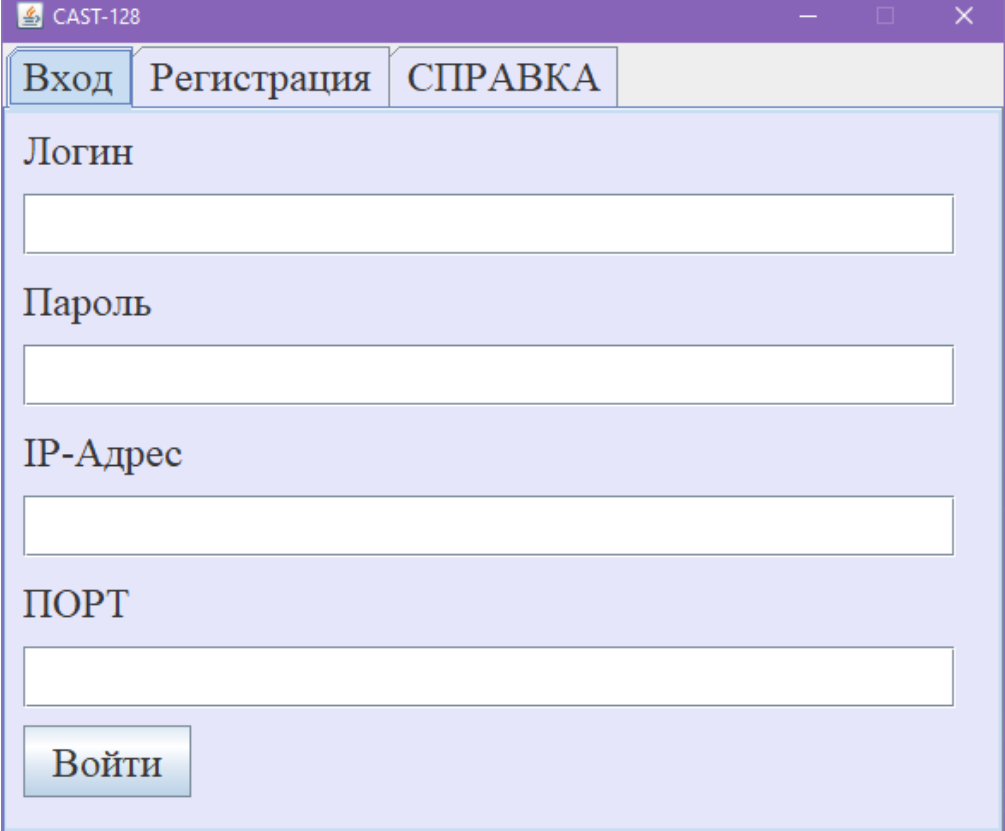
Вкладка справки:



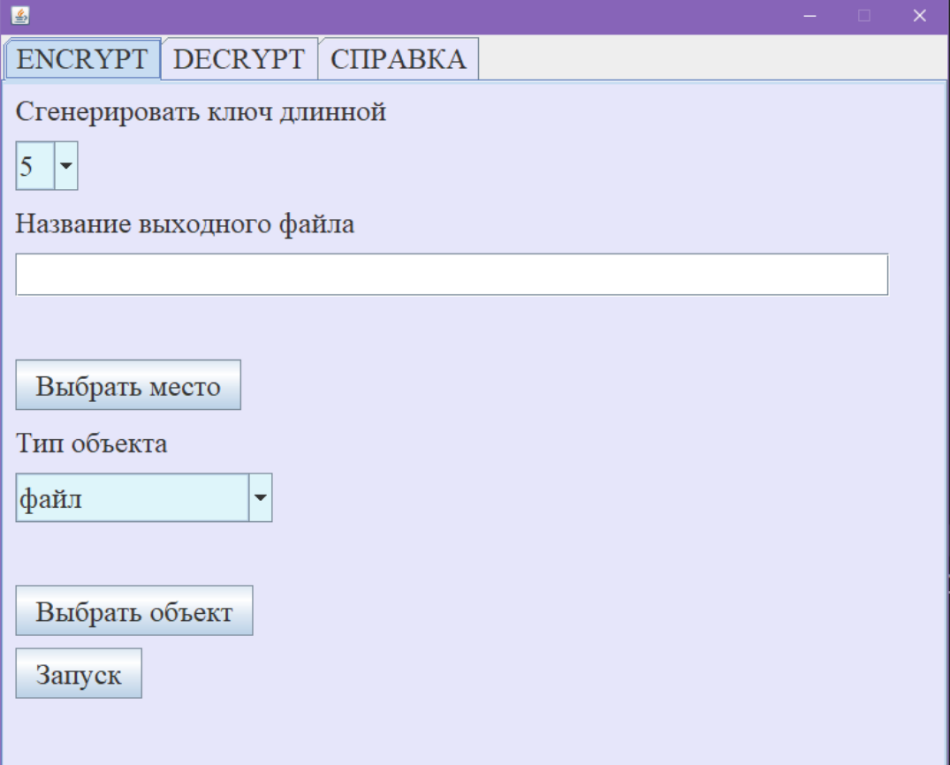
Интерфейс регистрации:



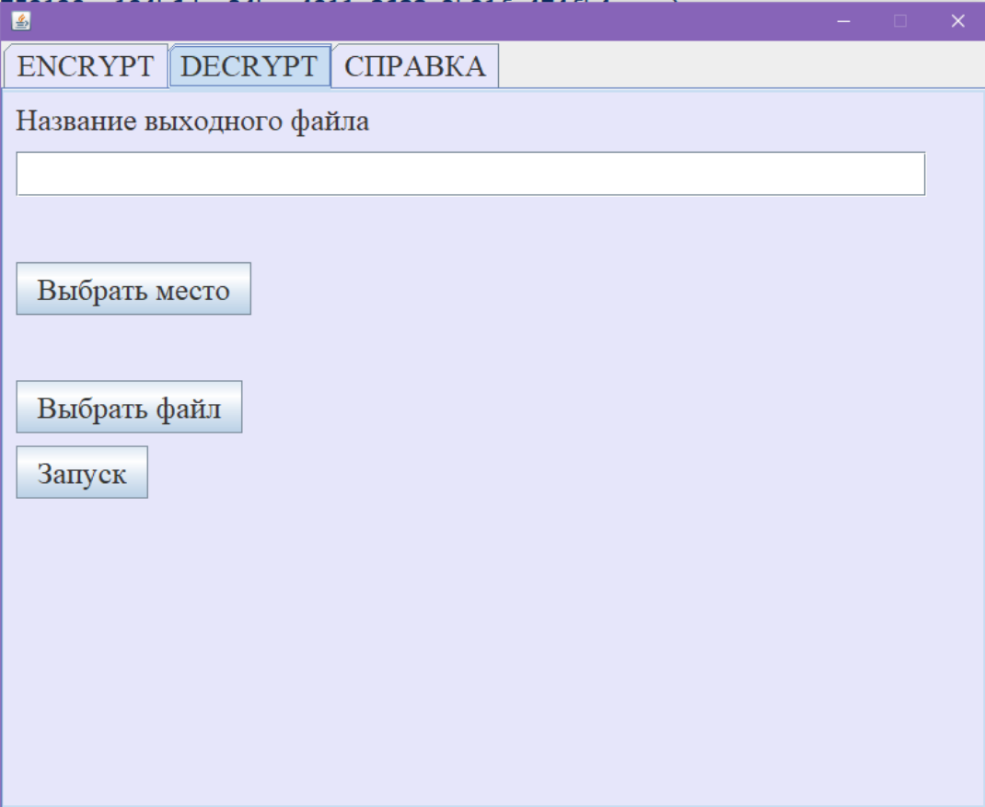
Интерфейс входа:



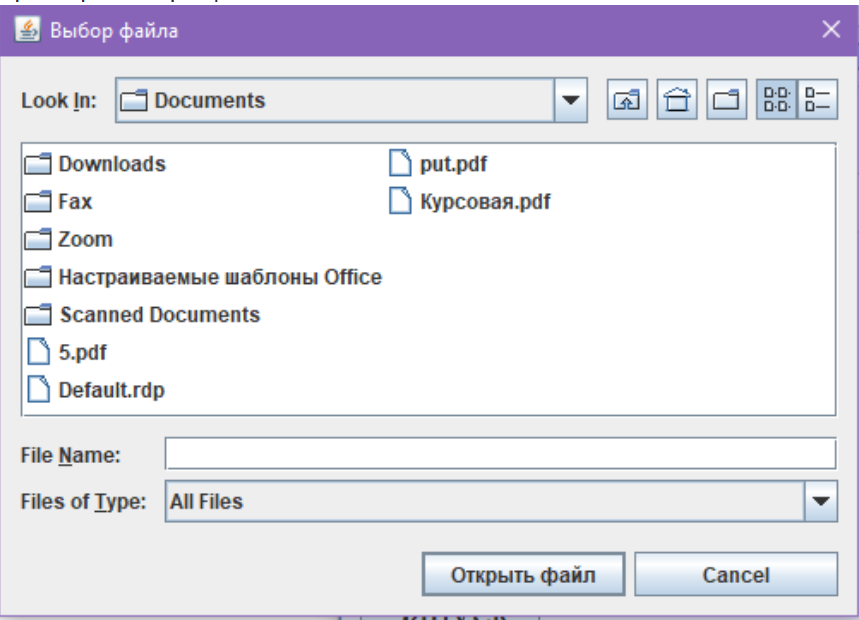
Вид интерфейса шифрования:



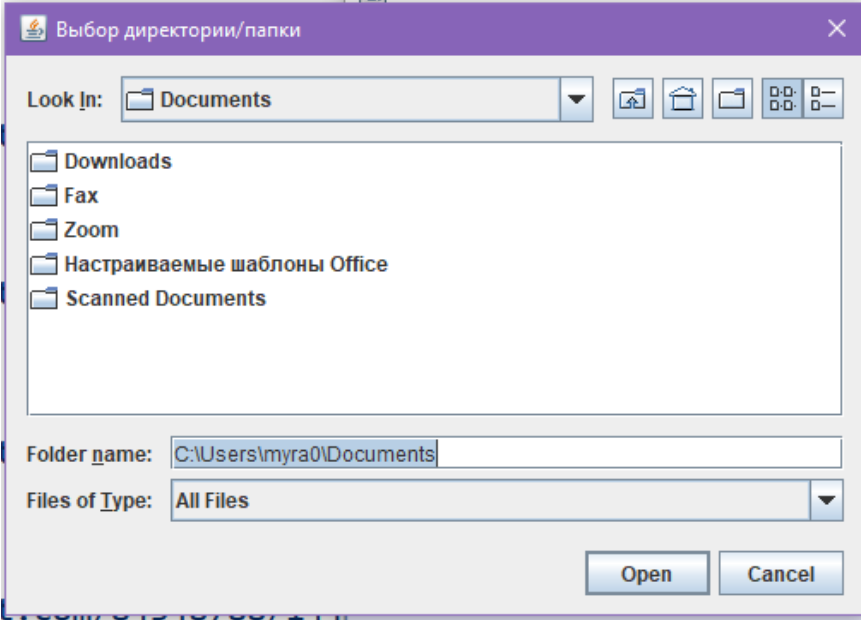
Вид интерфейса дешифрования:



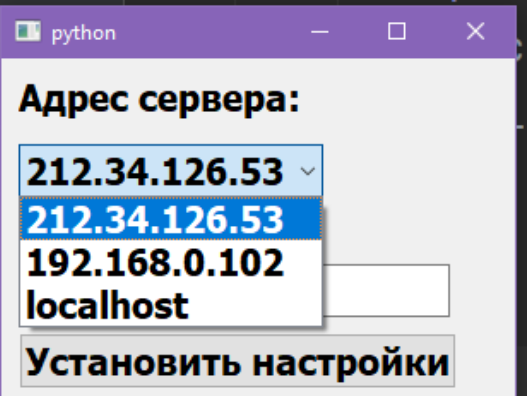
Пример выбора файла



Выбор папки:



Интерфейс сервера:



**Вывод:** В ходе лабораторной работы была реализована СКЗИ в клиент серверном исполнении, основанная на алгоритме CAST-128 с CBC. Видео работы программы, ее код и файлы доступны в репозитории по ссылке (https://github.com/Physalis-1/kripta)