Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»

(ВлГУ)

Кафедра ИЗИ

ОТЧЕТ

по лабораторной работе №3

по дисциплине «ПАСЗИ»

Тема: «Разработка и программная реализация криптографических алгоритмов»

|  |  |  |  |
| --- | --- | --- | --- |
| Студент гр. ИСБ-121 |  |  | Ходыкин Л.Ю. |
| Преподаватель |  |  | Тельный А.В. |

Владимир

2024

**Цель работы**

Изучение методов криптографической защиты данных.

**Задание**

* Реализовать программу осуществляющую шифрование (и дешифрование) файлов.

Способ/алгоритм шифрования выбирается самостоятельно. Рекомендуется, чтобы действия программы определялись через параметры командной строки.

Программа должна содержать справку, которая выдается при ее запуске без параметров.

В случае, если программе в качестве параметра не передан ключ (пароль), программа должна осуществлять его генерирование (пароль должен отвечать требованиям сложности, аналогично требованиям ЛР №1 по подгруппам).

**Реализация**

Для реализации используется ЯП Python3.12.

Требования к паролю:

 Наличие строчных и прописных латинских и кириллических букв.

 Наличие цифр и знаков препинания.

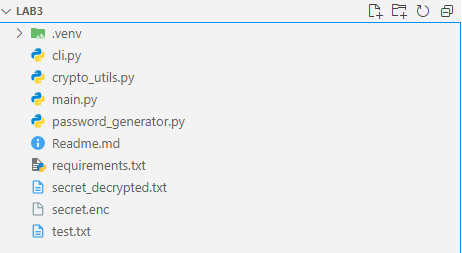
 Наличие символов арифметических операций.

 Отсутствие повторяющихся символов.

 Отсутствие подряд расположенных одинаковых символов.

 Несовпадение с именем пользователя, записанным в обратном порядке.

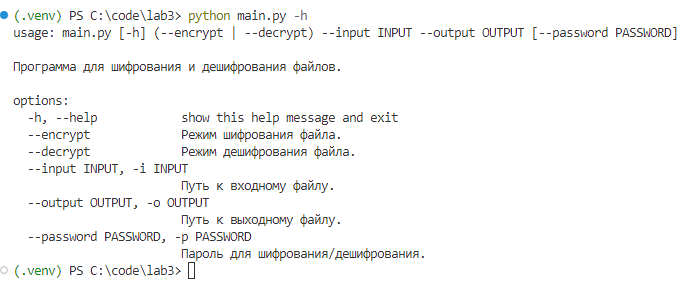
Структура проекта:



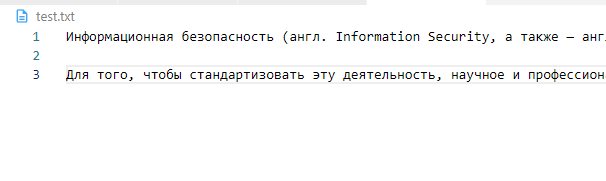
Для запуска программы необходимо ввести в терминал

python main.py -h

В результате в терминал выведется вспомогательная информация по использованию данной команды.



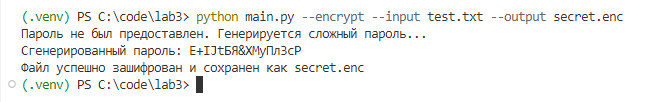
Создаем файл для шифрования с некоторым наполнением, который мы будем шифровать.



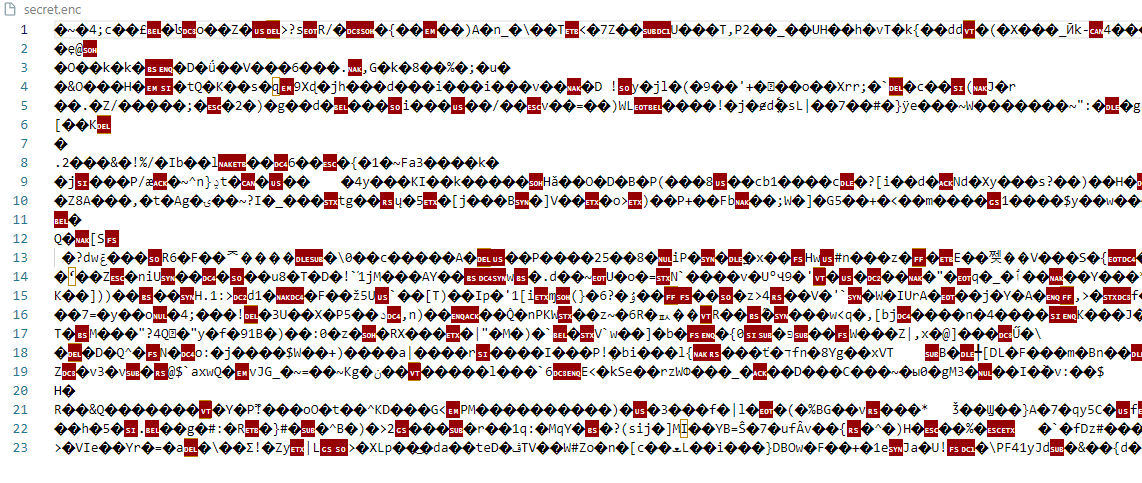
Сначала попробуем зашифровать файл с помощью автоматической генерации пароля. Для этого в терминал вводим команду.

python main.py --encrypt --input test.txt --output secret.enc

На выходе видно что пароль не был обнаружен и программа сгенерировала собственный пароль.



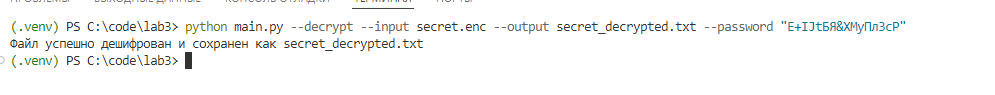
Содержание файла secret.enc



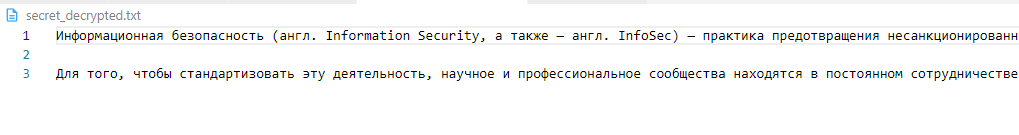
Для расшифровки введем в терминал следующую команду.

python main.py --decrypt --input secret.enc --output secret\_decrypted.txt --password "E+IJtБЯ&ХMуПл3cP"

В выводе видим, что файл успешно дешифровался и сохранен в новом файле.



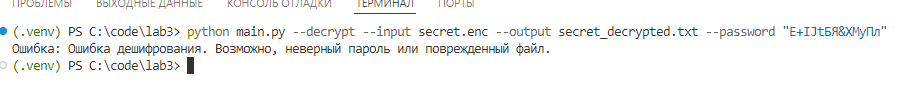
Наполнение расшифрованного файла.



Попробуем передать неправильный пароль. Для этого введем команду.

python main.py --decrypt --input secret.enc --output secret\_decrypted.txt --password "E+IJtБЯ&ХMуПл"

На выходе получим сообщение, что пароль не правильный или файл поврежден. Т.к. мы смогли расшифровать файл изначальным паролем, значит проблем с файлом нет.



Теперь попробуем повредить файл добавив новые строки и передать правильный пароль.

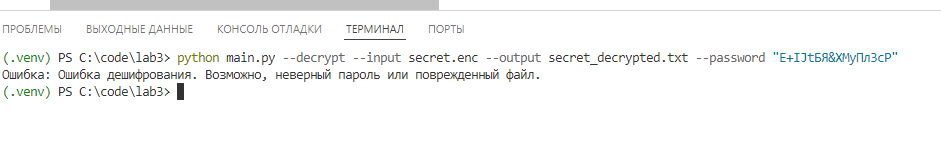
Измененный secret.enc



Вводим команду с правильным паролем

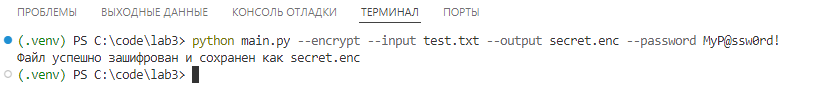
python main.py --decrypt --input secret.enc --output secret\_decrypted.txt --password "E+IJtБЯ&ХMуПл3cP"

На выходе видим ошибку



Теперь попробуем зашифровать с готовым паролем. Для этого вводим команду в терминал.

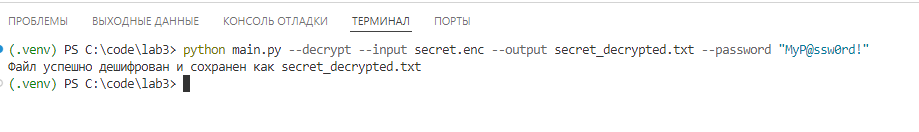
python main.py --encrypt --input test.txt --output secret.enc --password MyP@ssw0rd!



Видим, что файл успешно зашифровался и дополнительные пароли не генерировались.

Теперь попробуем расшифровать файл с тем же паролем. Для этого вводим команду в терминал.

python main.py --decrypt --input secret.enc --output secret\_decrypted.txt --password "MyP@ssw0rd!"

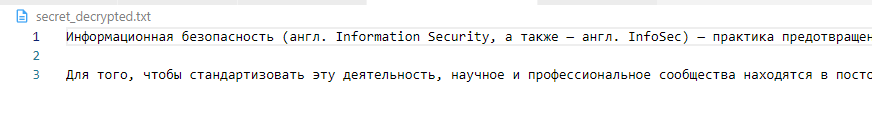


Файл успешно расшифровался.

Наполнение secret.enc



Наполнение secret\_decrypted.txt



Видно, что наполнение secret.enc поменялось в зависимости от пароля.

**Вывод:**

В результате проделанной лабораторной работы, я смог реализовать CLI скрипт, который может шифровать и дешифровать файл. Так же скрипт может генерировать пароль, если он не указан.