Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра интеллектуальных информационных технологий

Отчет по лабораторной работе №1

по курсу «СиМЗИИС»

Вариант 10

Выполнил студент

группы 121702: Колтович Д.С.

Проверил: Сальников Д.А.

**МИНСК**

2023

**Ход работы**

**Цель:** разработать программу реализующую следующие функции:

– Реализовать в виде программы шифр (зашифрование и расшифрование) в соответствии с вариантом. Язык исходного текста русский или английский по выбору исполнителя.

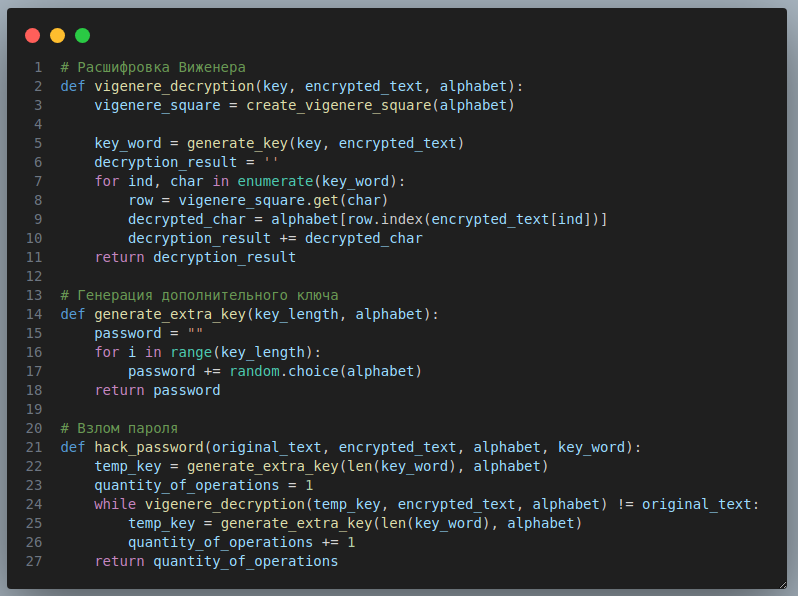
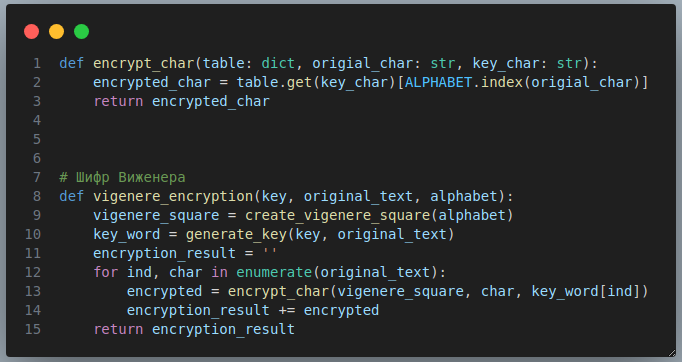
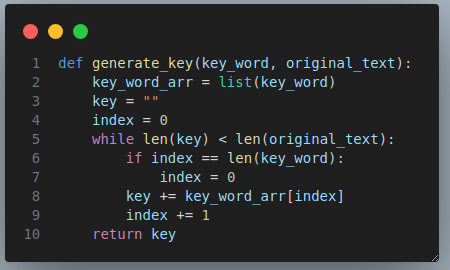
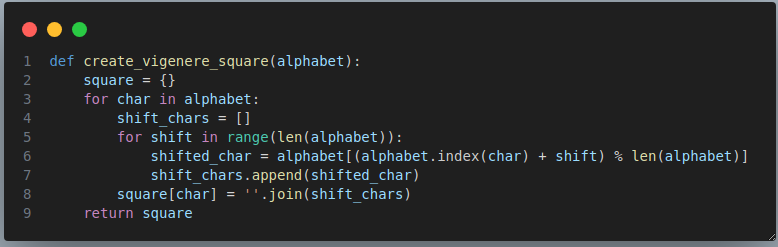
– Реализовать в виде программы атаку полным перебором ключа, используя для оценки правильности выбора ключа визуальный метод или исходный текст для автоматического сравнения результата дешифрования.;

– Оценить криптографическую стойкость реализованного шифра.

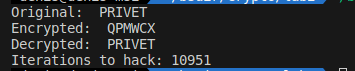
– Предложить варианты усложнения шифра. Предложенные варианты оформить в виде алгоритма..

**Выполнение:**

**Исходный код программы:**



1. **Вывод программы:**



1. **Вариант алгоритма усложнения шифрования**
   1. Шифруем текст шифром Цезаря с указанным сдвигом
   2. Шифруем полученный текст шифром Винежера с кодовым словом Х1
   3. Снова шифруем текст шифром Цезаря с другим сдвигом
   4. Шифруем текст шифром Винежера с кодовым словом Х2

**Вывод:**

В ходе проделанной работы была разработана программа, реализующая все поставленные функции, предложен вариант усложнения шифрования. Была оценена криптографическая стойкость шифра Винежера для конкретного текста и ключа.