Министерство образования

Республики Беларусь

Учреждение образования

Белорусский государственный университет

информатики и радиоэлектроники

Кафедра: интеллектуальных информационных технологий

Отчёт

По дисциплине

«Средства и методы защиты информации в интеллектуальных системах»

Тема: «Простейшие криптографические преобразования»

Написал: Проверил

Германенко В.В., гр. 321701 Сальников Д. А.

Минск 2025

Цель: освоить базовые шифры, узнать их применение, сильные и слабые стороны

Задача:

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

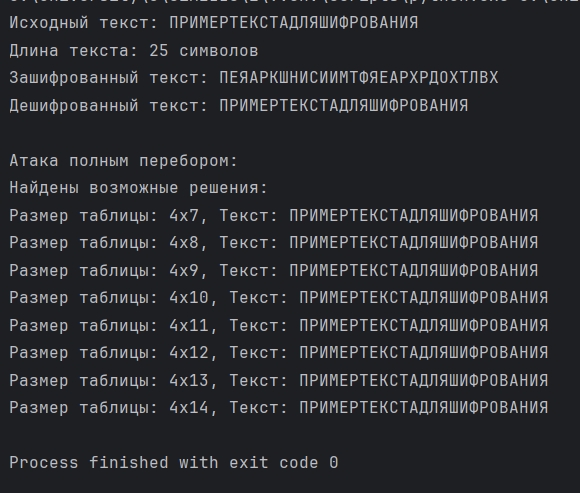
2) Реализовать в виде программы атаку полным перебором ключа, используя для оценки правильности выбора ключа визуальный метод или исходный текст для автоматического сравнения результата дешифрования.

3) Оценить криптографическую стойкость реализованного шифра.

4) Предложить варианты усложнения шифра. Предложенные варианты оформить в виде алгоритма.

4) Шифр перестановки, использующий простые (прямоугольные) таблицы.

Работа программы:



Практические рекомендации:

На основе проделанной работы можно сделать вывод, что шифр перестановки, использующий прямые таблицы слишком слаб для применения его на практике, слишком малое количество возможных ключей.

Вывод: освоил базовые шифры и научился понимать их слабые стороны.