|  |
| --- |
|  |

Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение

высшего образования

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ

МОРДОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

им. Н.П. ОГАРЁВА»

(ФГБОУ ВО «МГУ им. Н.П. Огарёва»)

Институт электроники и светотехники

Кафедра информационной безопасности и сервиса

ЛАБОРАТОРНАЯ РАБОТА №7

по теме:

«Шифрование с помощью аналитических

преобразований»

Автор отчёта о лабораторной работе  А. Е. Конышев

подпись, дата

Обозначение лабораторной работы ЛР–02069964–02.03.02–08–23

Направление подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Проверил работу

канд. техн. наук, доц.  И. П. Карьгин

подпись, дата

Саранск 2023

**Шифрование с помощью аналитических преобразований с использованием перемножения матрицы на вектор.**

Если матрицу использовать в качестве ключа, а вместо компонента вектора подставить символы текста, то компоненты вектора будут представлять собой символы зашифрованного текста.

Алгоритм шифра заключается в следующем:

1. Выбирается квадратная матрица с определителем отличным от 0 (для ускорения шифрации выбирается размерность от 3 до 5);
2. Символы исходного текста переводятся в десятичное представление (например, можно использовать позицию в алфавите или код символа в любой кодировке);
3. Переведенный текст разбивается на блоки, равные размерности матрицы, последний блок забивается любыми символами по необходимости;
4. Матрица перемножается с каждым блоком разбиения, полученные результаты записываются в новый числовой вектор;

Этот вектор – есть шифр.

Алгоритм дешифрации производит аналогичные преобразования, но с другой, обратной матрицей и вектором:

1. Вычисляется матрица, обратная к ключу шифра
2. Исходный шифр разбивается на блоки по длине равные размерности матрицы;
3. Матрица, полученная из первого пункта, перемножается на блоки из второго пункта
4. Полученные результаты можно переводить сразу, а можно записывать в новый вектор, который необходимо перевести в символьное представление с использованием того же алгоритма, что и при шифровании.

Результат работы программы с данными и текстом представлен на рисунке 1.

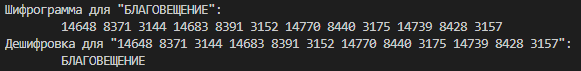


Рисунок 1 – Результат работы программы.