

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИ ЛАБОРАТОРНОЙ РАБОТЫ №4**

**В РАМКАХ ДИСЦИПЛИНЫ «МЕТОДЫ И СРЕДСТВА КРИПТОРГАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»**

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

1. Зашифровать (расшифровать) вводимый с клавиатуры текст и тексты, открываемые из файлов.

Шифрование текста вводимого с клавиатуры

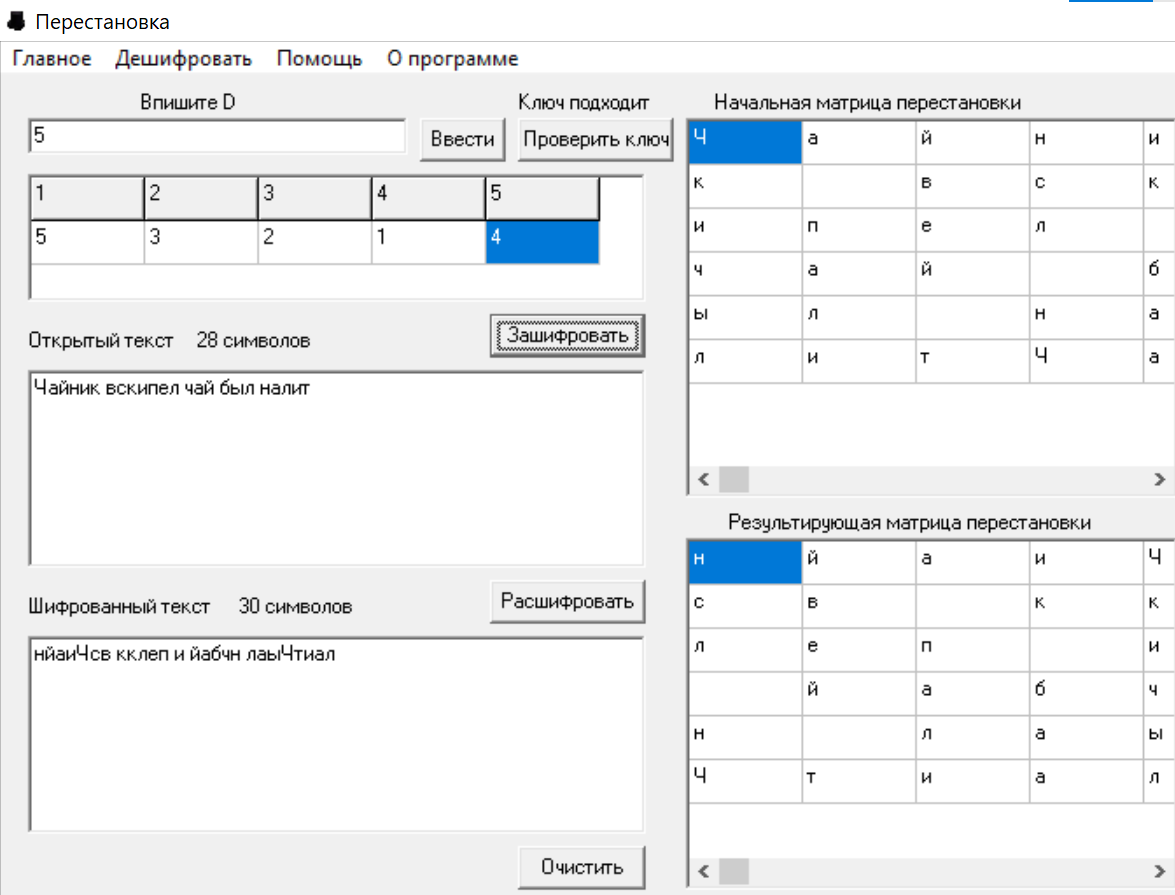


Рисунок 1 - Шифрование текста вводимого с клавиатуры

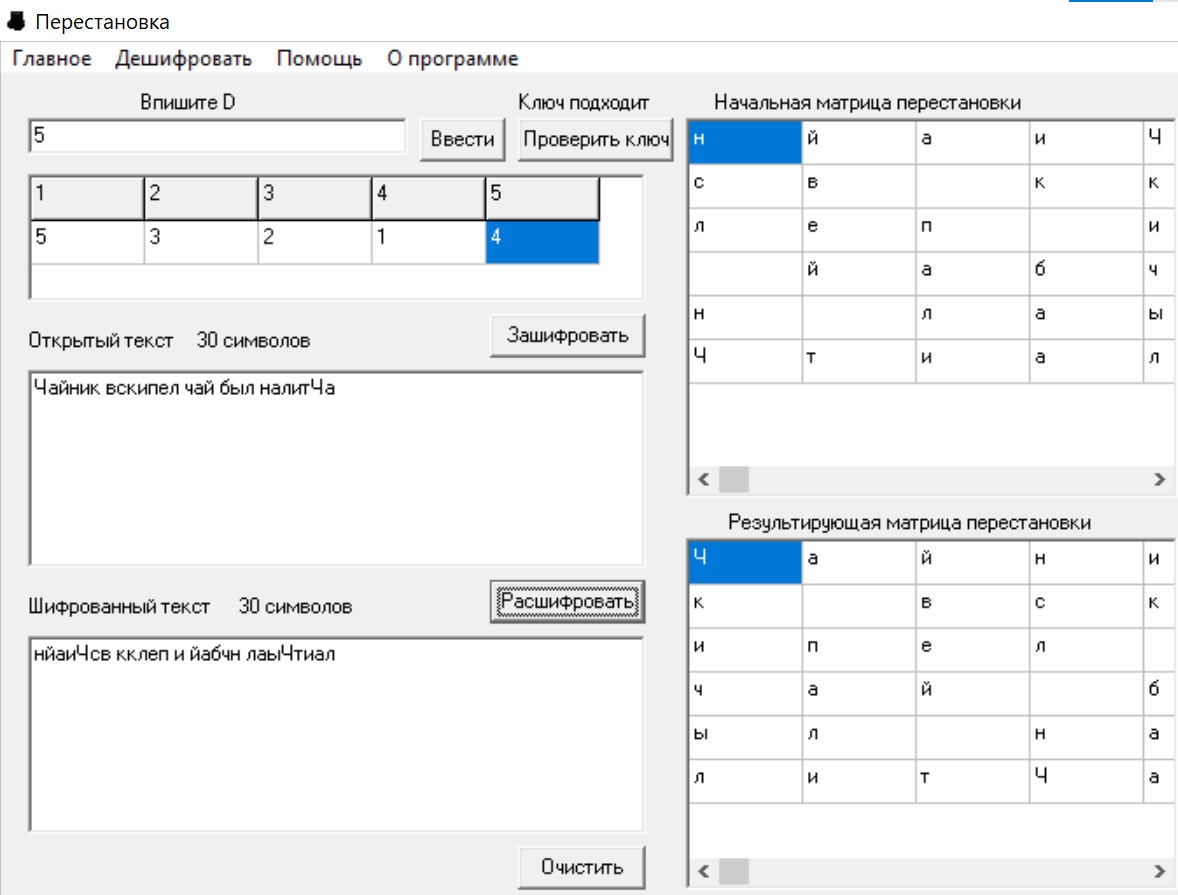


Рисунок 2 - Дешифрование введенного текста

Можно заметить, что для шифрования текста, в случае, когда символов текста не хватает для полного блока, до заполнение идет циклически (с первого символа)

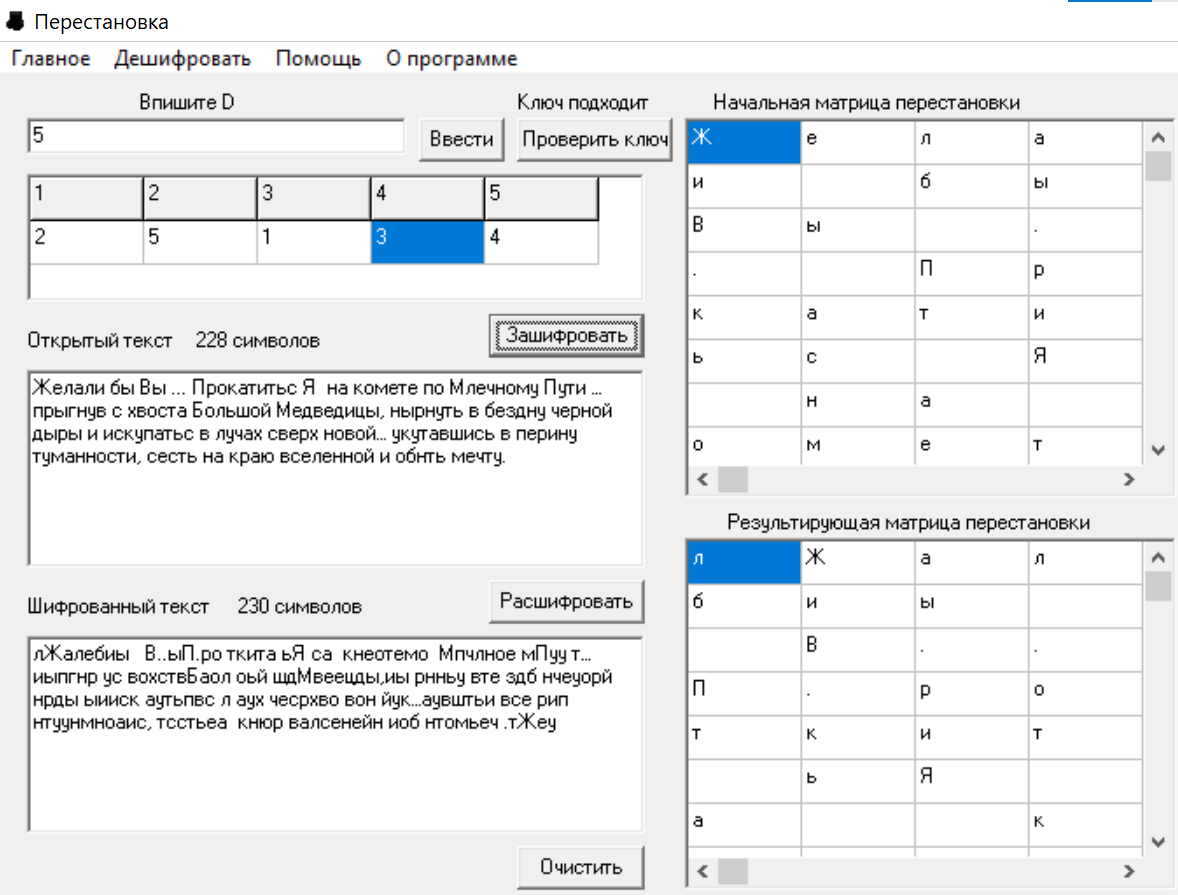


Рисунок 3 - Шифрование тестового текста

2. Произвести попытку дешифрования данных, зашифрованных в п. 1 (если попытка вскрытия криптограмм не удалась, сделать выводы о причинах неудачи). Привести в отчете экранные формы.

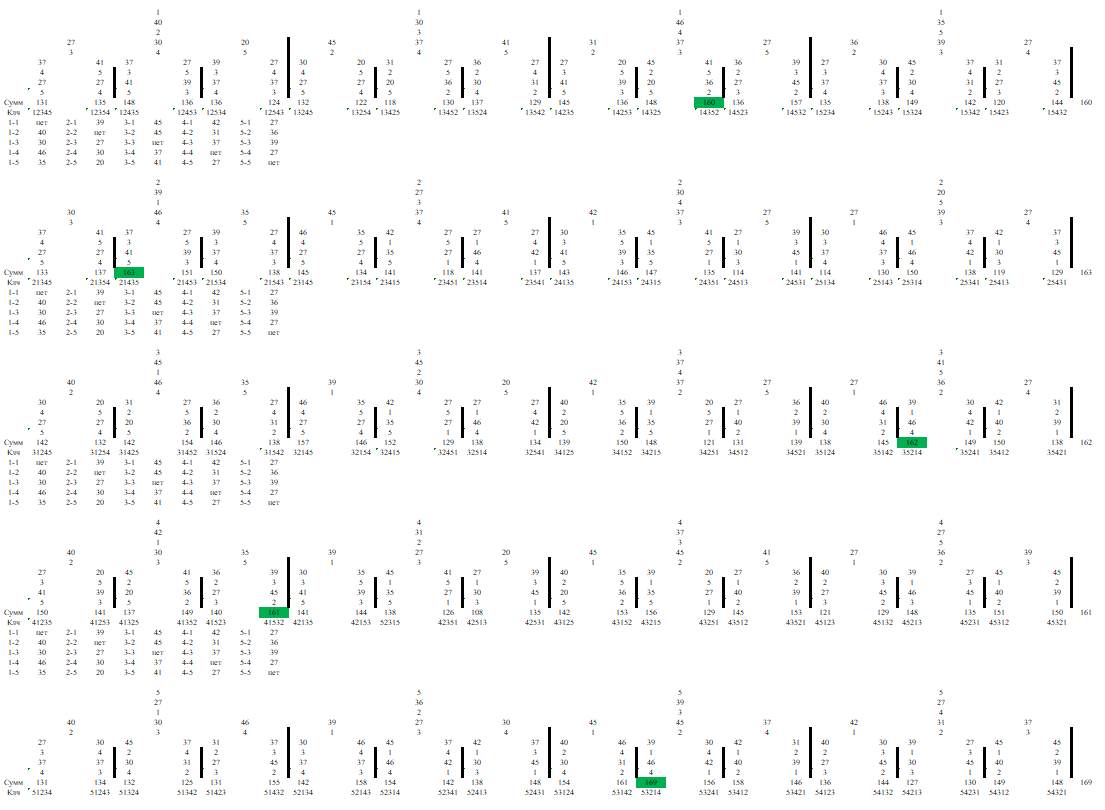
Используя таблицу биграмм из приложения сложим суммы вероятности биграмм в столбцах.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| н | й | а | и | Ч |
| с | в |  | к | к |
| л | е | п |  | и |
|  | й | а | б | ч |
| н |  | л | а | ы |
| Ч | т | и | а | л |

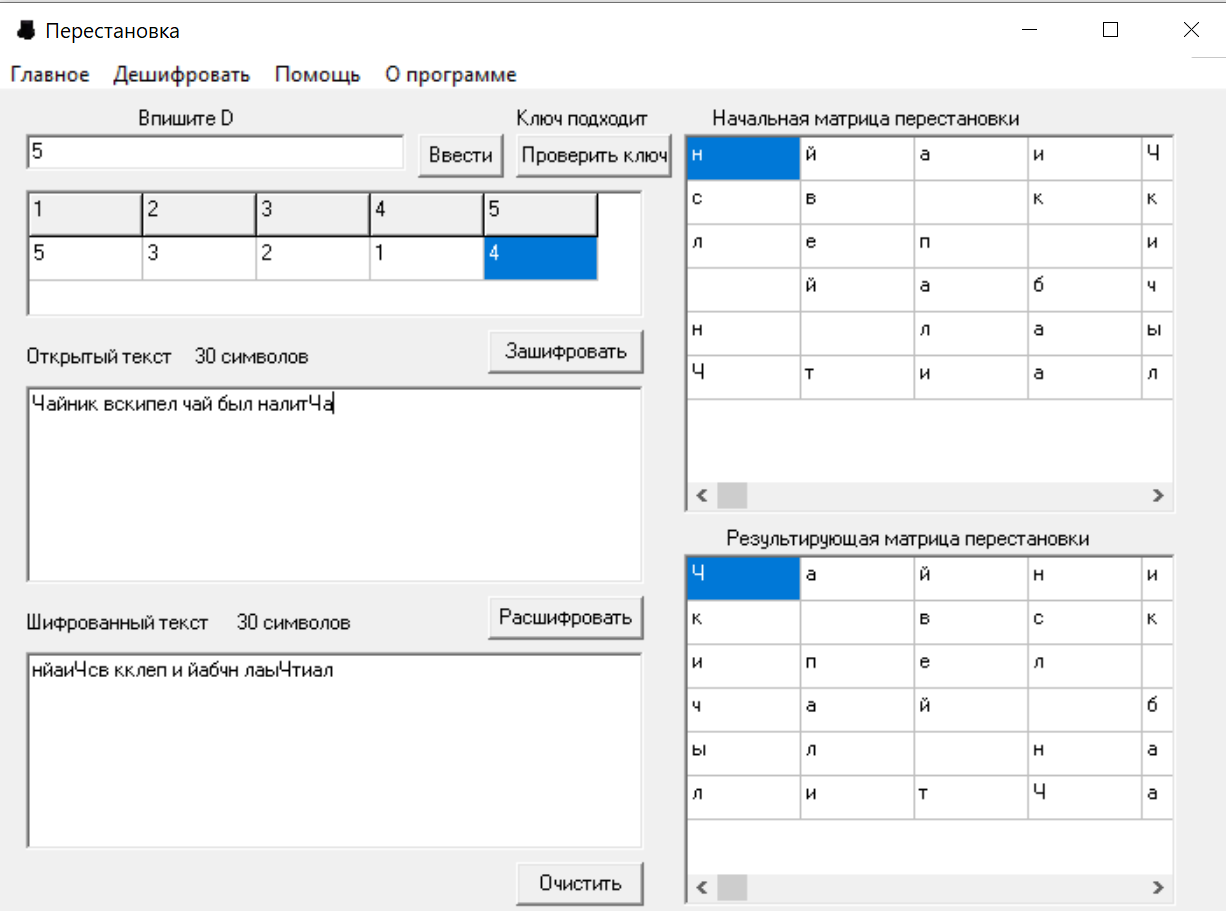
Таблица 1 – Результирующая матрица перестановки

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1-1 | нет | 2-1 | 39 | 3-1 | 45 | 4-1 | 42 | 5-1 | 27 |
| 1-2 | 40 | 2-2 | нет | 3-2 | 45 | 4-2 | 31 | 5-2 | 36 |
| 1-3 | 30 | 2-3 | 27 | 3-3 | нет | 4-3 | 37 | 5-3 | 39 |
| 1-4 | 46 | 2-4 | 30 | 3-4 | 37 | 4-4 | нет | 5-4 | 27 |
| 1-5 | 35 | 2-5 | 20 | 3-5 | 41 | 4-5 | 27 | 5-5 | нет |

Построим дерево решений.



Как видно из рисунка максимальное значение (169) принимает ключ 53214. Попробуем расшифровать сообщение с его помощью.



Дешифровка удалась. Ключ 53214