

**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

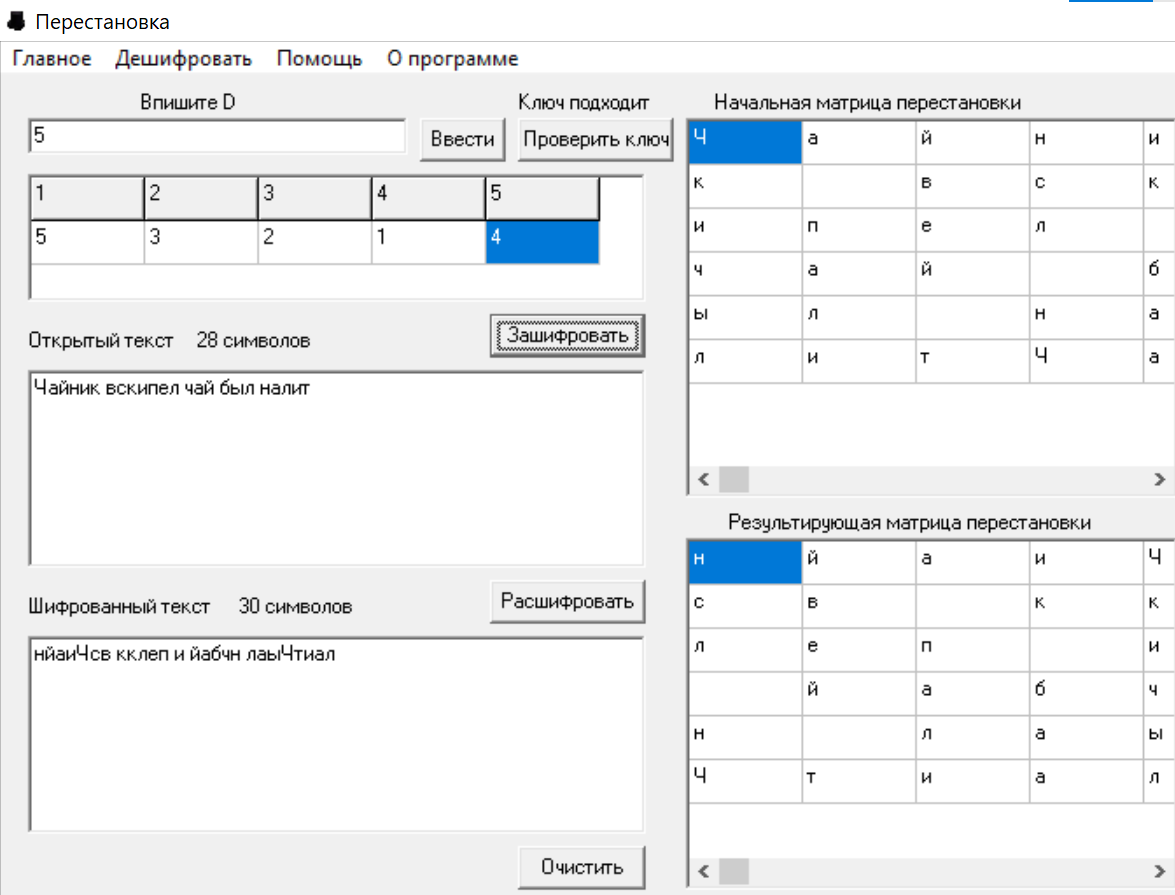


Рисунок 1 - Шифрование текста вводимого с клавиатуры

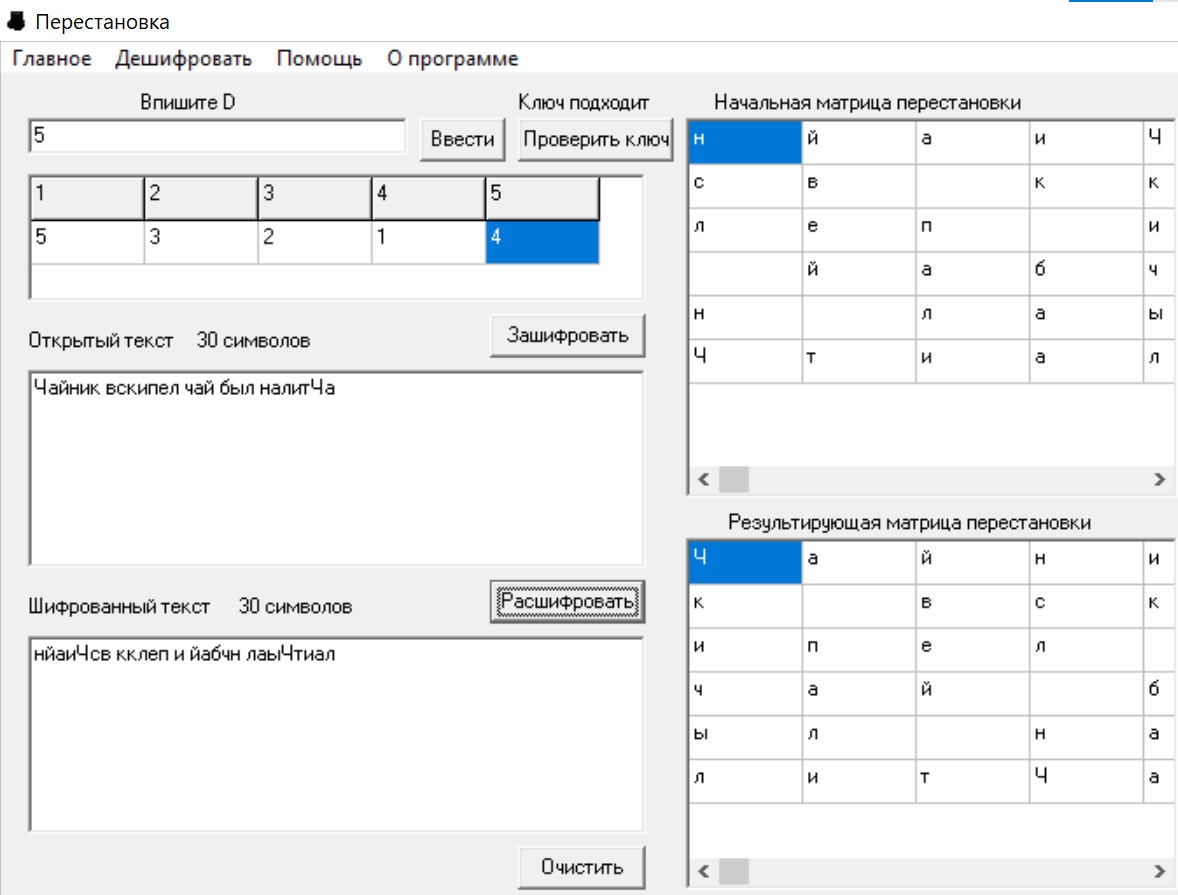


Рисунок 2 - Дешифрование введенного текста

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

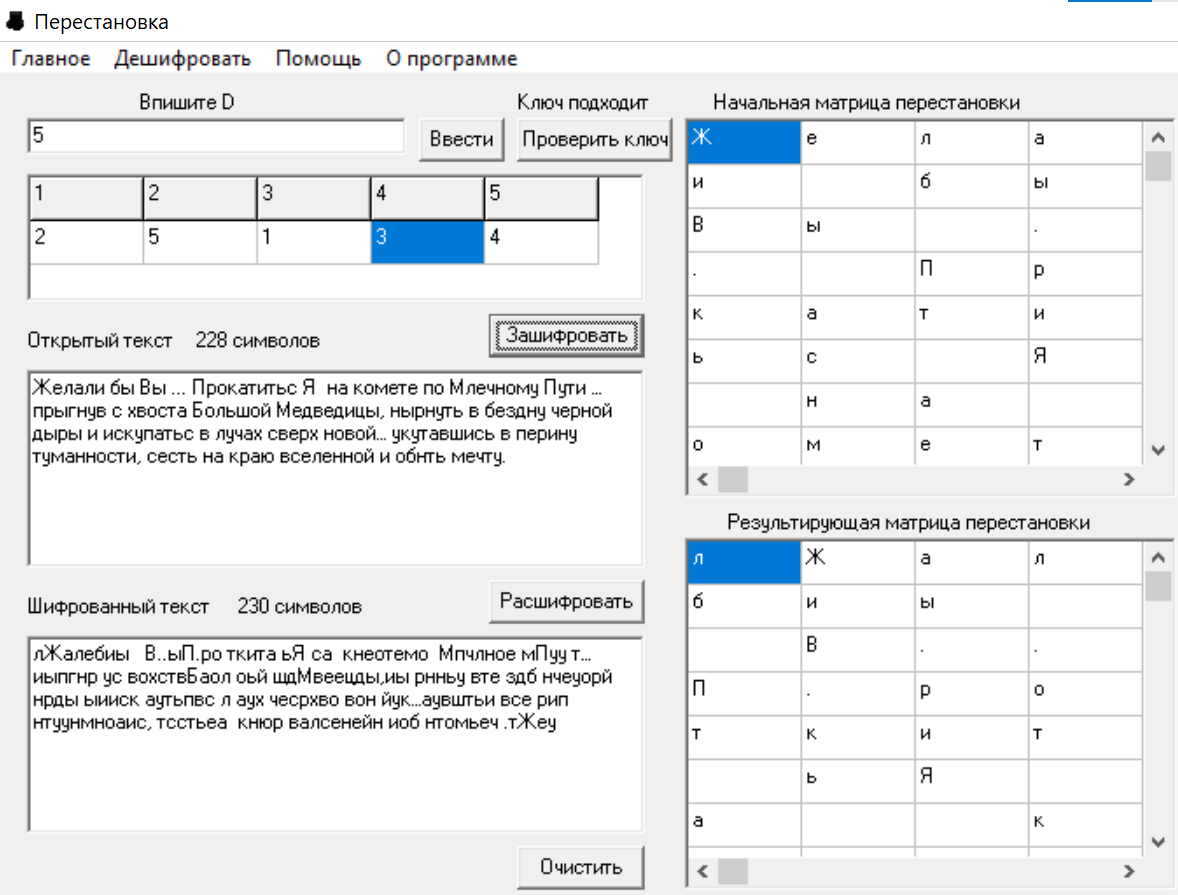


Рисунок 3 - Шифрование тестового текста

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

1-2 = нй+св+ле+ й+н +чт = 40

1-3 = иа+с +лп+ а+нл+чи =20

1-4 = ни+ск+л + б+на+ча = 46

1-5 = нч+ск+ли+ ч+ны+чл = 27

2-1 = йа+вс+ел+й + н+тч = 35

2-3 = йа+в +еп+йа+ л+ти =27

2-4 = йи+вк+е +йб+ а+та =30

2-5 = йч+вк+еи+йч+ ы+тл =20

3-1 = ан+ с+пл+а +лн+ич =45

3-2 = ай+ в+пе+ай+л +ит =43

3-4 = аи+ к+п +аб+ла+иа =37

3-5 = ач+ к+пи+ач+лы+ил =41

4-1 = ин+кс+ л+б +ан+ач =46

4-2 = ий+кв+ е+бй+а +ат = 36

4-3 = иа+к + п+ба+ла+аи =41

4-5 =ич+кк+ и+бч+аы+ал =25

5-1 = чн+кс+ил+ч +ын+лч =24

5-2 = чй+кв+ие+чй+ы +лт =24

5-3 = ча+к +ип+ча+ыл+ли = 39

5-4 = чи+кк+и +чб+ыа+ла =27



Исходя из вероятностей перестановки попробуем получить ключ.

Первый столбец исходной матрицы переместился на 4 место.

Второй столбец мог переместиться на все места кроме 4, и по таблице скорее всего переместился на первое место, однако на первое место так же могли переместиться и 3, и 4, и 5 столбец. Среди перемещений по вероятности лидирует перемещение 4-1, то есть второй столбец не переместился ни на первое, ни на 4 место (т.к. на 4 переместился первый столбец). В таком случае второй столбец мог переместиться на 3 и на 5 место. Однако так как 4 уже на первом, то сравнивать нужно вероятности второго и 5 столбца, где 5 более высокая вероятность, тогда методом исключения подучаем что 2 столбец перемещается на 5 позицию, а 5 на 3. Соответственно 3 столбец перемещается на 2 позицию.

Таким образом получим ключ 43512

Дешифровка текста не удалась, так как исходный текст не является настолько объемным, чтобы в нем работали вероятностные характеристики.

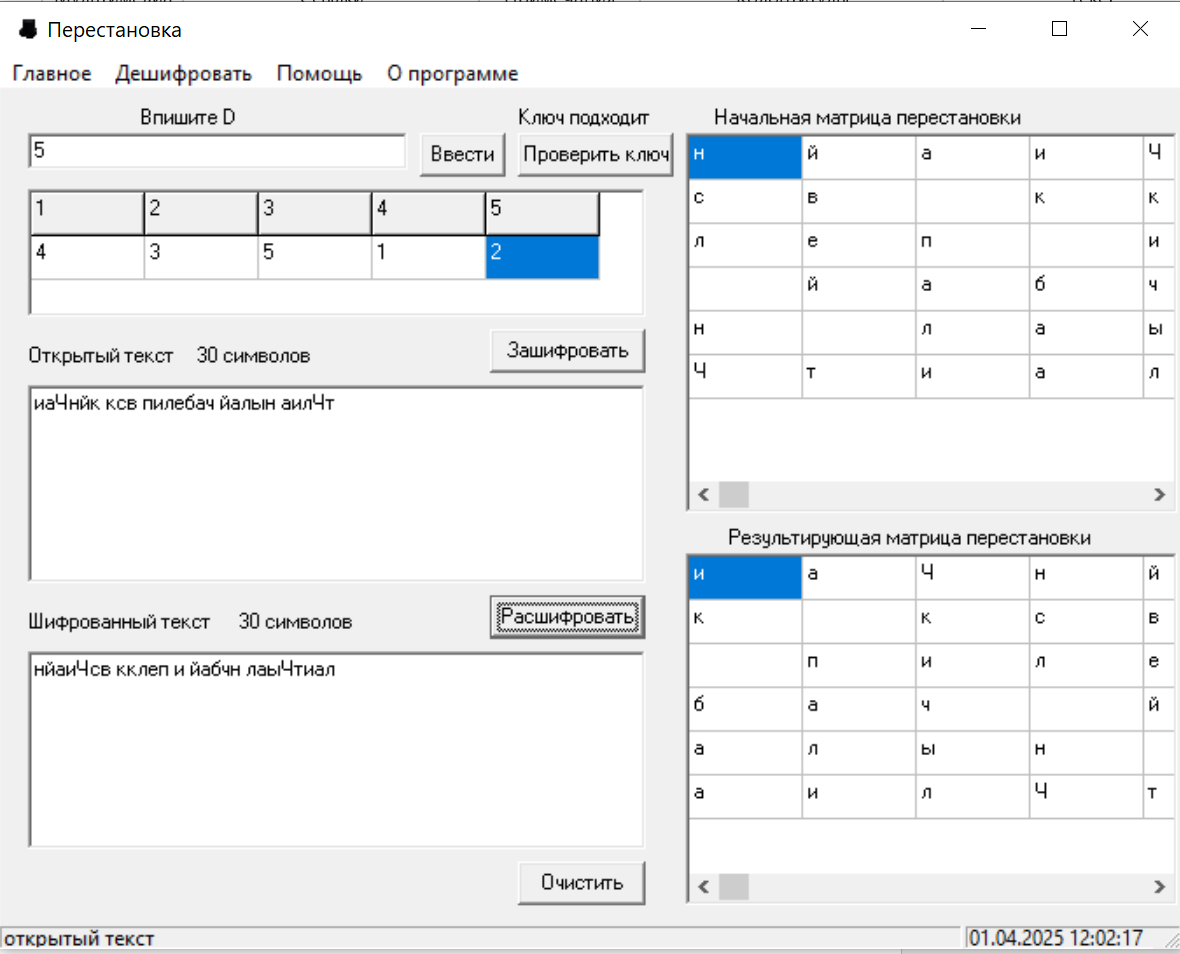


Рисунок 4 - Попытка дешифрования текста подобранным ключом

3. Добиться правильного дешифрования зашифрованного текста (подбором длины и содержания исходного текста, длины ключа шифрования). Приложить экранные формы, сделать выводы об особенностях исследуемого метода вскрытия криптограмм.

Анализируя текст, можно заметить заглавные буквы. Возьмем первые 5 букв нйфиЧ. Очевидно, что буква Ч должна стоять на первом месте. То есть идет перестановка 5-1. Далее пользуясь вероятностной таблицей, можно однозначно определить, что 1 символ перешел на 4 позицию (перестановка 1-4). Далее обратим внимание на 3 символ, он может стоять на позициях 1 и 4, тогда по вероятностной таблице он переходит на позицию 2 (перестановка 3-2). Теперь смотрим на 4 столбец. Он не может быть на позициях 1,2, соответственно он на позиции либо 3, либо 5. Однако на 3 позицию претендует так же и 2 столбец, у которого вероятность находиться на этом месте немного выше, что дает возможность предположить перестановку 2-3 и 4-5 соответственно. Таки образом получаем полный список перестановок 5-1, 2-3, 3-2, 4-5 и получаем исходный ключ 53214.

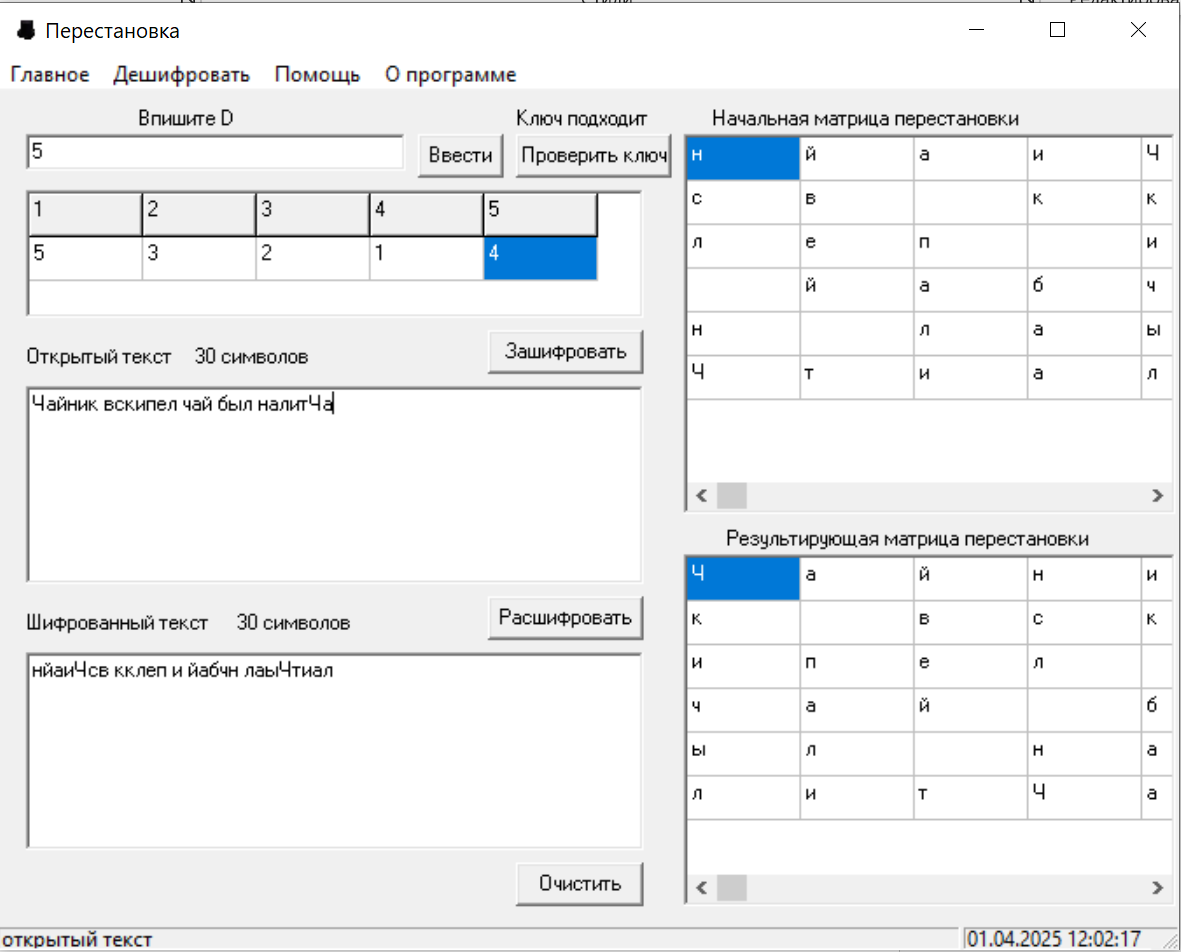


Рисунок 5 - Результат дешифровки с новым ключом