Министерство науки 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. Огарева)

Факультет довузовской подготовки и
среднего профессионального образования
Выпускающая предметная цикловая комиссия общепрофессиональных и
специальных (информационно-коммуникационных) дисциплин

ОТЧЕТ ПО ЛАБОРАТОРОНОЙ РАБОТЕ №2

по дисциплине: «Информационная безопасность»

ИССЛЕДОВАНИЕ РАЗЛИЧНЫХ МЕТОДОВ ЗАЩИТЫ ТЕКСТОВОЙ ИНФОРМАЦИИ И ИХ СТОЙКОСТИ НА ОСНОВЕ ПОДБОРА КЛЮЧЕЙ

Автор практической работы _____ Н.С. Потапов

подпись, дата

Обозначение практической работы ПР-02069964-09.02.07-14-23

Направление подготовки 09.02.03 Программирование в компьютерных системах

Руководитель работы
преподаватель _____ П.В. Венчаков

подпись, дата

Саранск 2023

Цель работы: изучение методов шифрования (расшифрования) перестановкой символов, подстановкой, гаммированием, использованием таблицы Виженера. Исследование и сравнение стойкости различных методов на основе атак путем перебора всех возможных ключей.

Ход работы:

1. Выполнил настройку программы: запустил программу, создал текстовый файл «text», в файле написал текст, для дальнейшей работы с ним. Затем выбрал метод шифрования «Замена» со сдвигом «2». Выполненная работа представлена на рисунке 1.

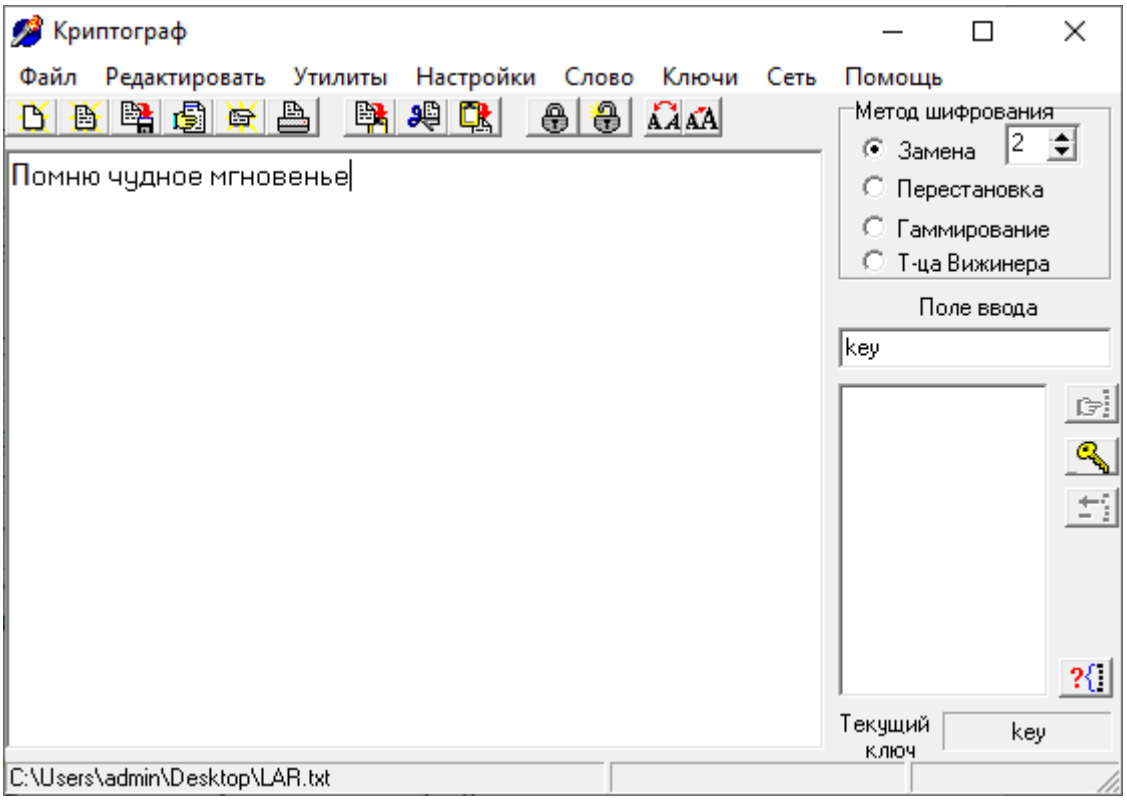

Рисунок 1 – Исходный текст

2. Нажал кнопку «Зашифровать файл», подтвердил своё действие в открывшемся окне и получил зашифрованный текст. Выполненная работа представлена на рисунке 2.

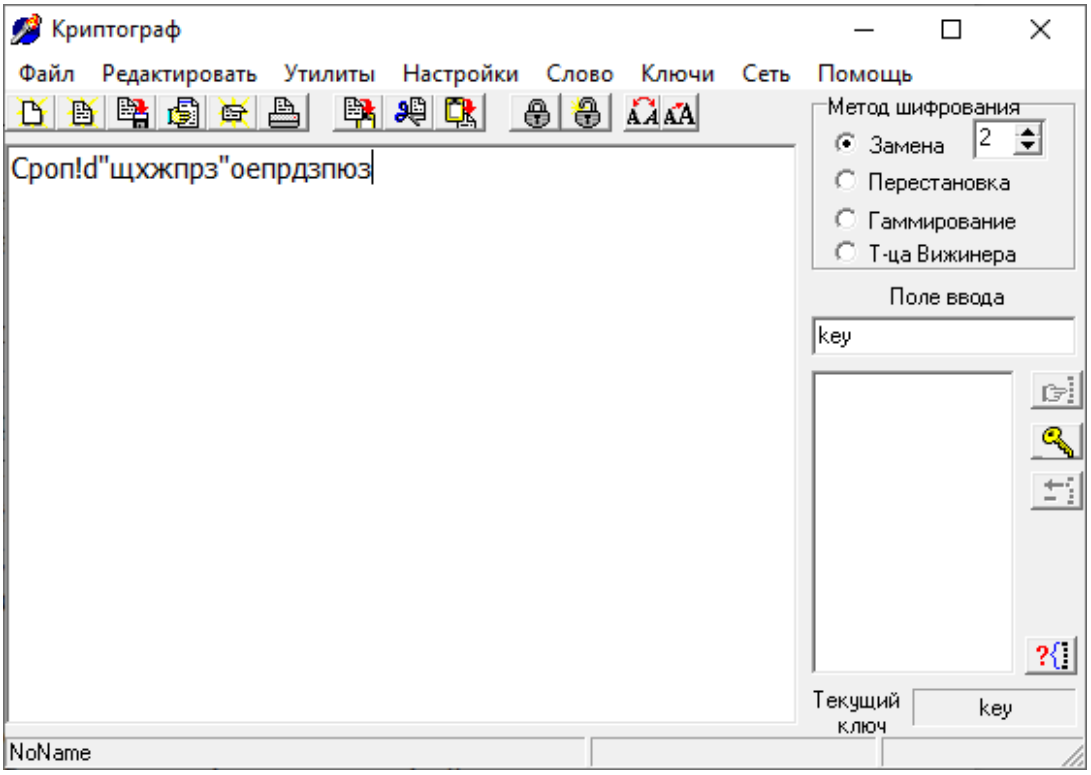

Рисунок 2 – Зашифрованный текст методом «Замена»

3. Для того, чтобы расшифровать текст выполнил следующие действия: сохранил файл, ввёл вероятное слово, выбрал метод шифрования «Замена», после чего нажал кнопку «Run». Когда закончится подбор, мы получим ключ шифрования и расшифрованный текст. Выполненная работа представлена на рисунке 3 – 4.

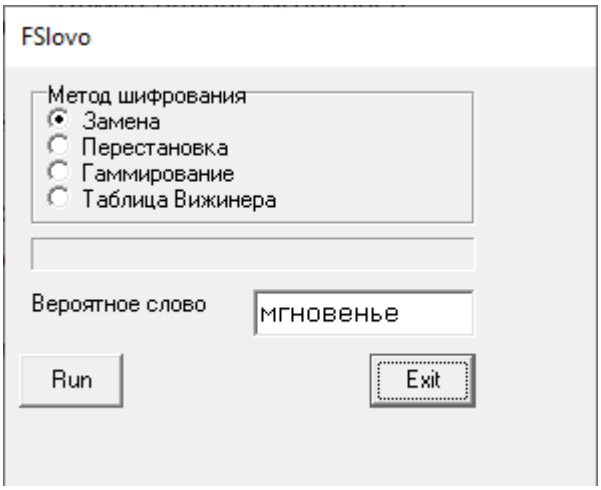

Рисунок 3 – Ввод вероятного слова

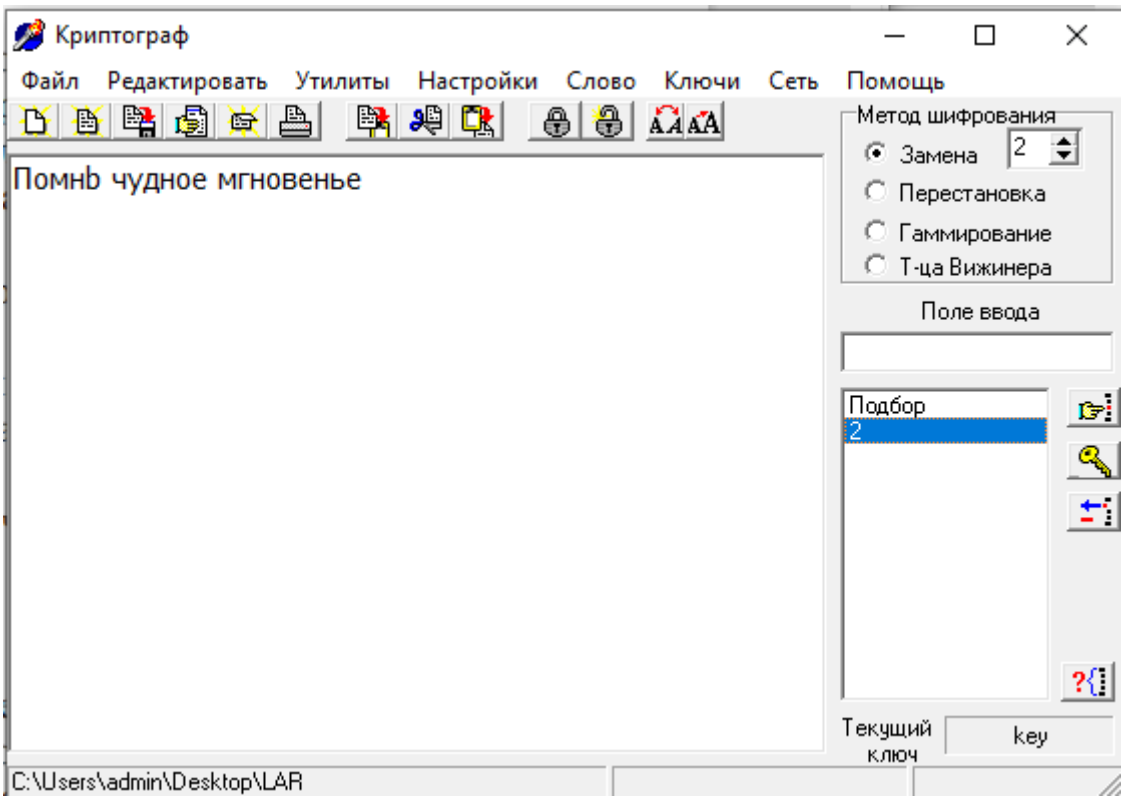

Рисунок 4 – Дешифрованный текст

4. Указал метод шифрования «Перестановка», в открывшемся окне выбрал длину ключа «3», с комбинацией – 312. Выполненная работа представлена на рисунке 5 – 6.

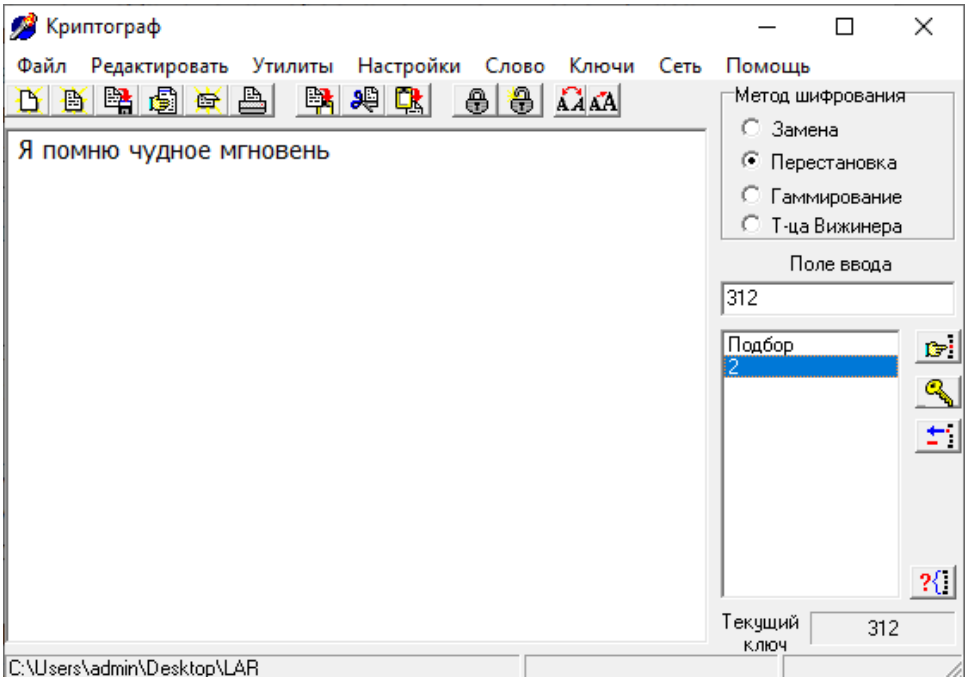

Рисунок 5 – Настройка ключа

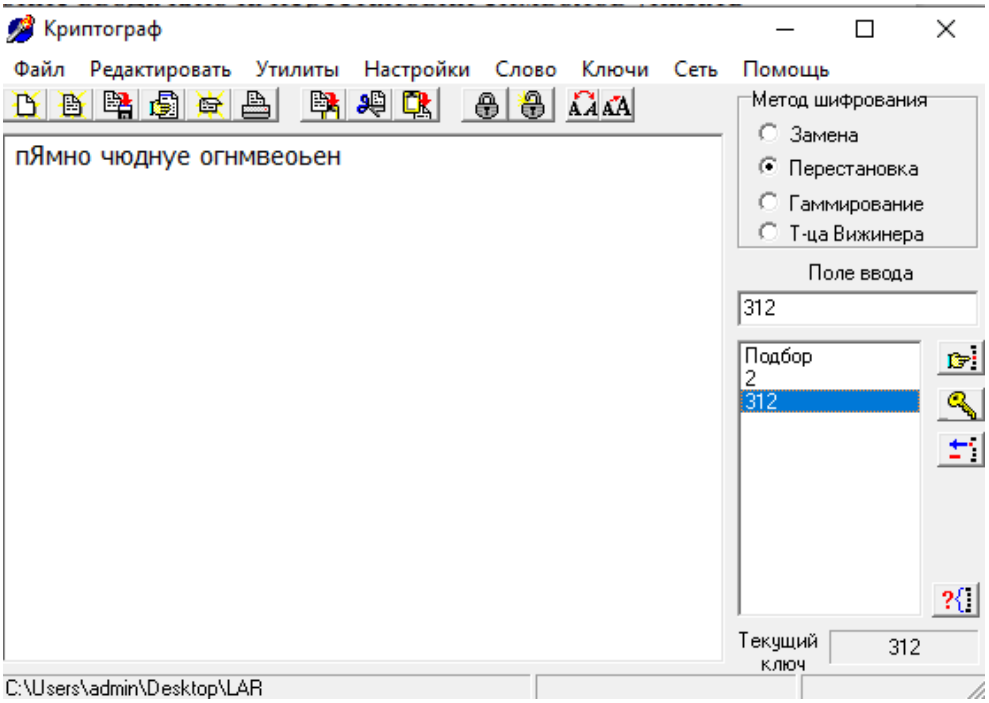

Рисунок 6 – Зашифрованный текст

5. Дешифровку выполнял также как предыдущем пункте, получил исходный текст. Выполненная работа представлена на рисунке 7.

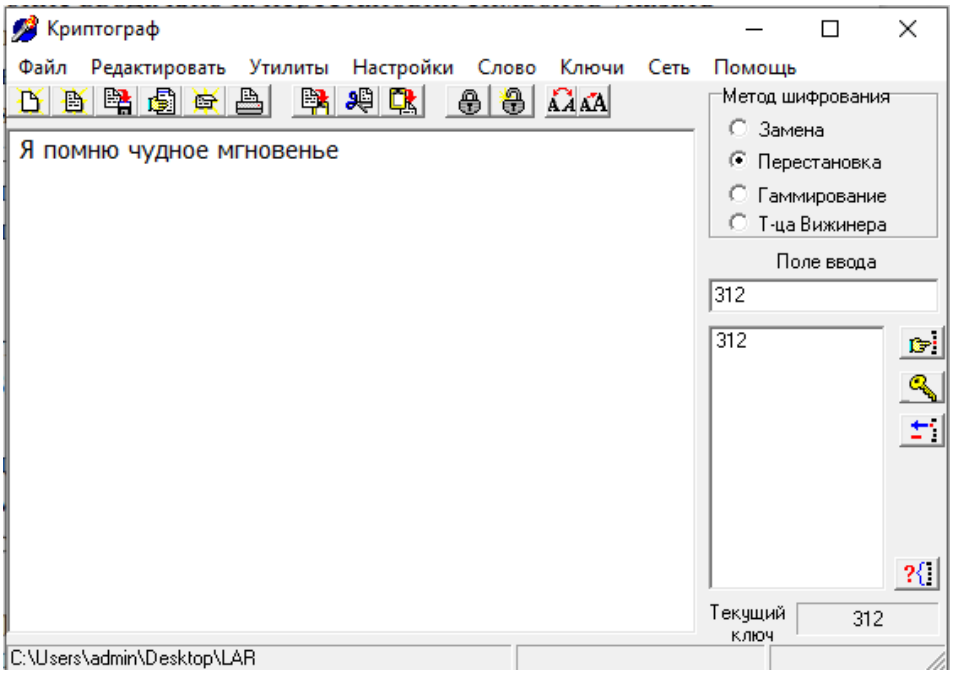

Рисунок 7 – Исходный текст

6. Для шифрования выбрал «Гаммирование» и нажал «Зашифровать файл. Выполненная работа представлена на рисунке 8.

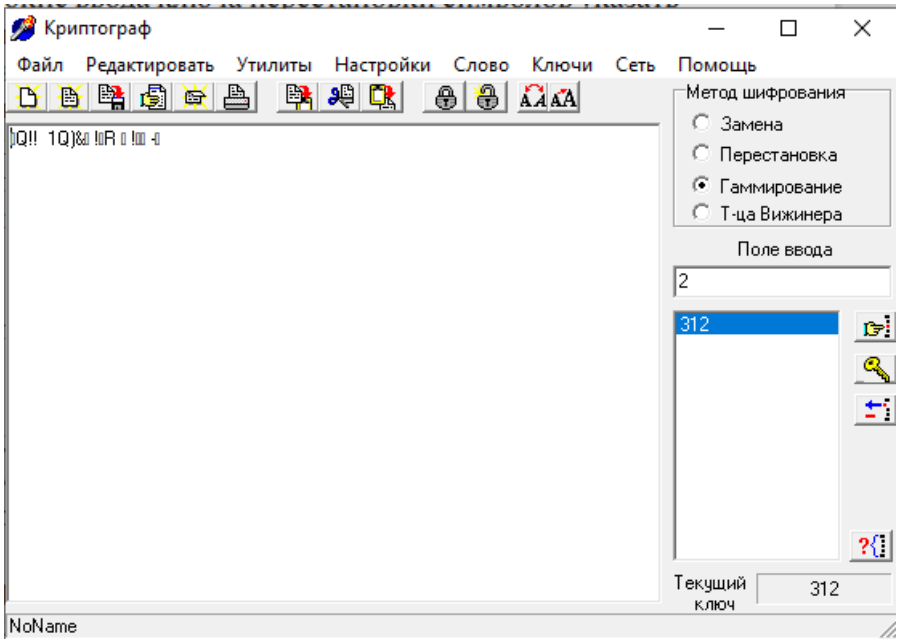

Рисунок 8 – Метод гаммирования

7. При выполнении дешифрации повторил шаги как в предыдущих пунктах. Получил исходный текст без ошибок, все верно.

8. Выбрал метод шифрования «таблица Виженера» и нажал «Зашифровать файл», Выполненная работа представлена на рисунке 9.

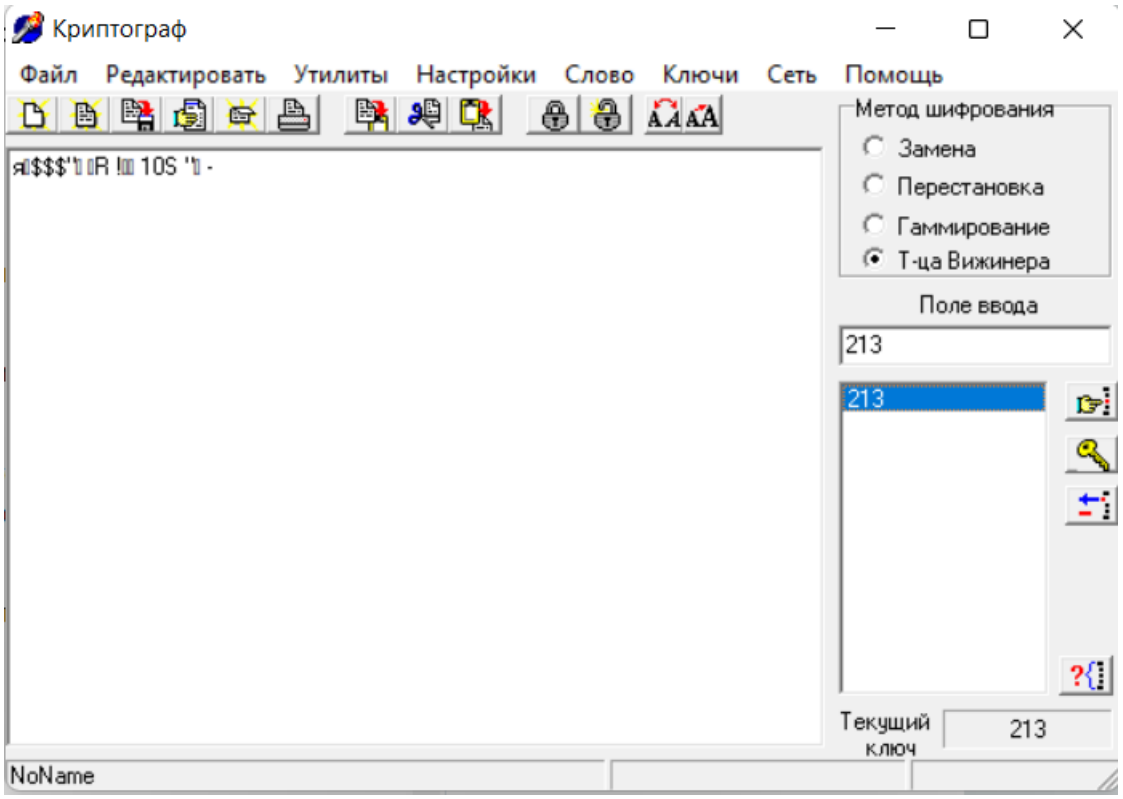

Рисунок 9 – Таблица Виженера

Ответ на контрольный вопрос – 14 вариант:

В чем недостатки метода дешифрования с использованием протяжки вероятного слова?

1. Требует знания хотя бы одного верного слова.
2. Ограничен поиском на основе вероятных слов.
3. Эффективность зависит от длины слова.
4. Неустойчив к ошибкам в предполагаемом слове.