

**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 №2**

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

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

ЗубаревВ.С.

**Шифрование заменой со сдвигом**

При шифровании заменой со сдвигом задается сдвиг по таблице ASCII 1251 по формуле Тш=(То+K)mod256, где K –величина сдвига.

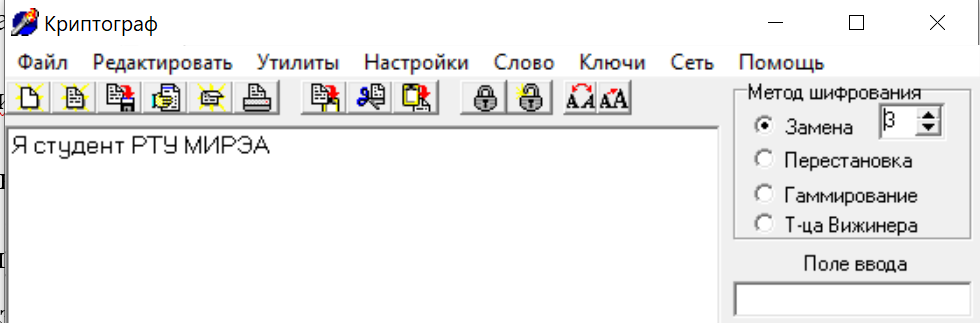


Рисунок 1 - Открытый текст

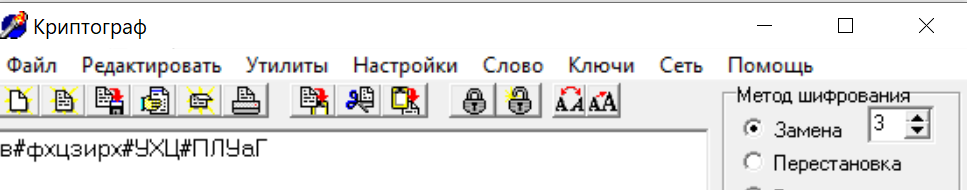


Рисунок 2 – Зашифрованный текст

**Шифрование методом перестановки**

При шифровании методом перестановки текст разбивается на блоки, равные длине ключа (в случае если блок не полный он дополняется пробелами), внутри которого происходит перестановка символов согласно ключу. То есть если ключ 3412, то первый символ в блоке открытого текста встанет на третье место в блоке шифрованного текста, второй- на четвертое, третий на первое, четвертый – на второе.

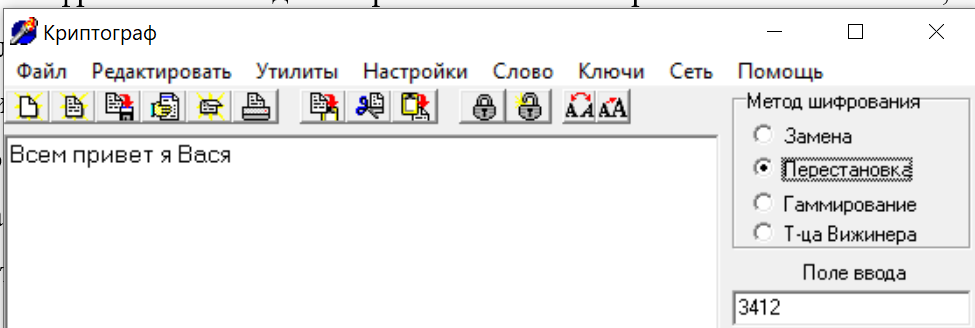


Рисунок 3 – Открытый текст

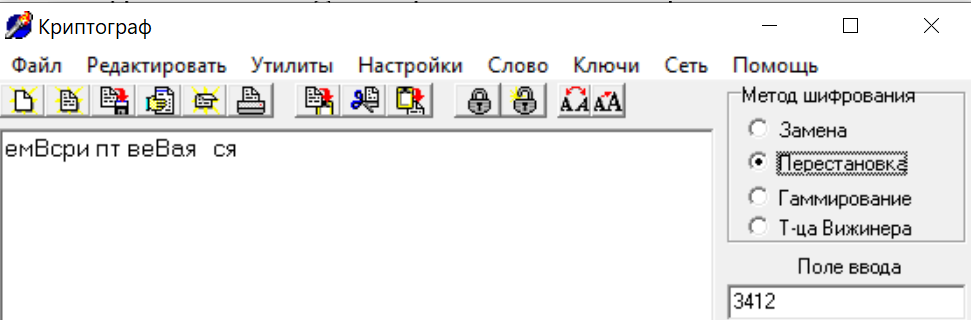


Рисунок 4 – Зашифрованный текст

**Шифрование методом гаммирования**

В данном методе шифрования используется операция побитного сложения по модулю 2 (XOR). На блок открытого текста побитово накладывается блок гаммы (произвольных значений). В случае если блок гаммы больше, чем блок открытого текста, блок гаммы обрезается.

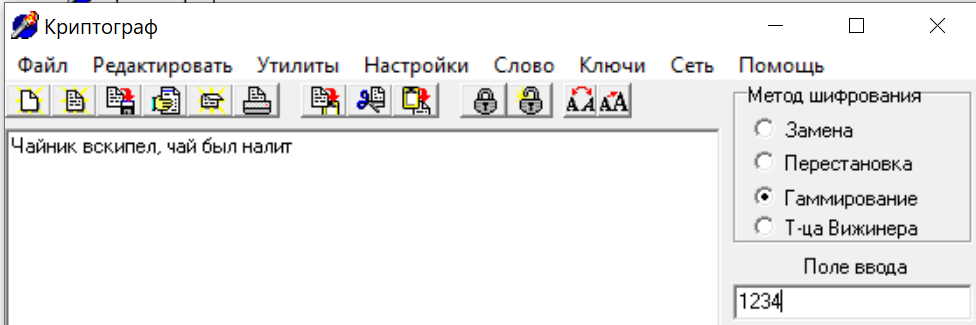


Рисунок 5 – Открытый текст

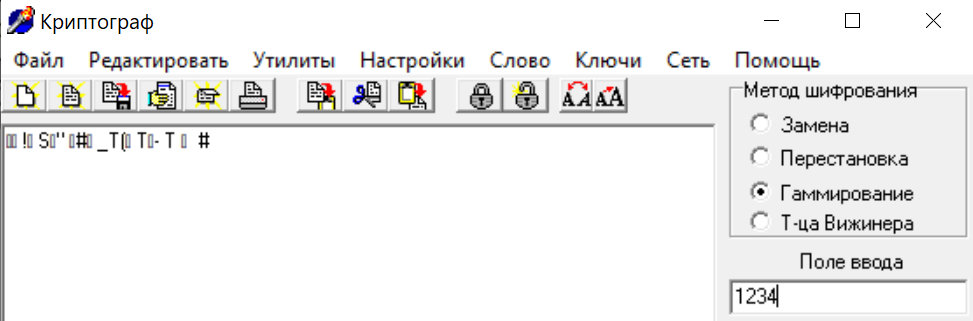


Рисунок 6 – Зашифрованный текст

**Метод шифрования по таблице Вижинера**

В данном методе шифрования используется таблица Вижинера размером NxN, где N – мощность алфавита. Таблица представляет собой алфавит, где каждая следующая строчка сдвигает алфавит на 1 влево. То есть первая строчка таблицы это алфавит записанный полностью в правильном порядке, следующая строчка – это алфавит где место каждого символа в строчке сдвинулось на 1 влево (например для русского алфавита для буквы В позиция в первой строке будет 3, на второй строке 2, на третьей 1, а на 4 она станет 33) Шифрование происходит при помощи ключа (слова), которое повторяется посимвольно пока последовательность не станет равна длине сообщения. Шифрование происходит путем замены символов открытого текста по правилу Тш= T[То,Тк]. В таблице Вижинера ищется пересечение символа ключа и символа открытого текста, и символ их пересечения и будет символом зашифрованного текста.

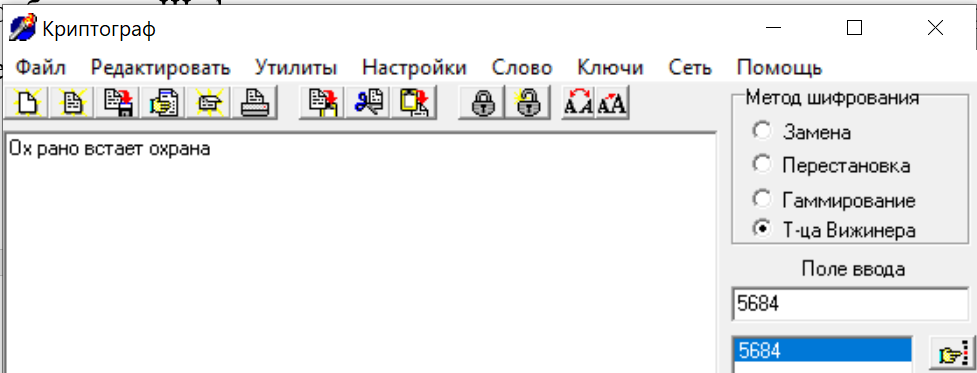


Рисунок 7 – Открытый текст

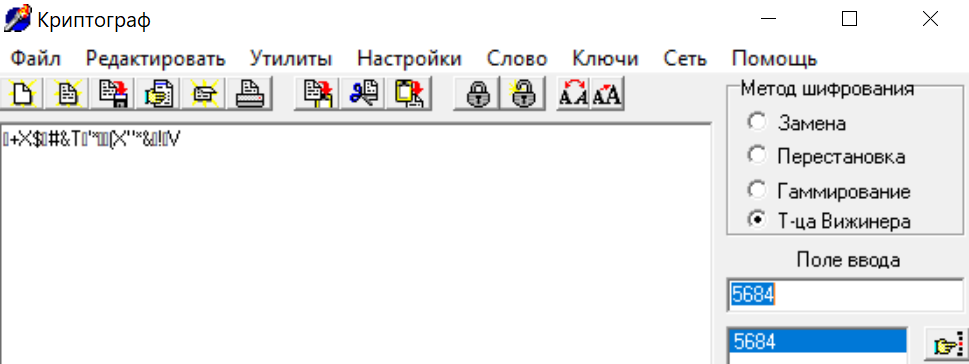


Рисунок 8 – Закрытый текст

**Дешифрование замены со сдвигом**

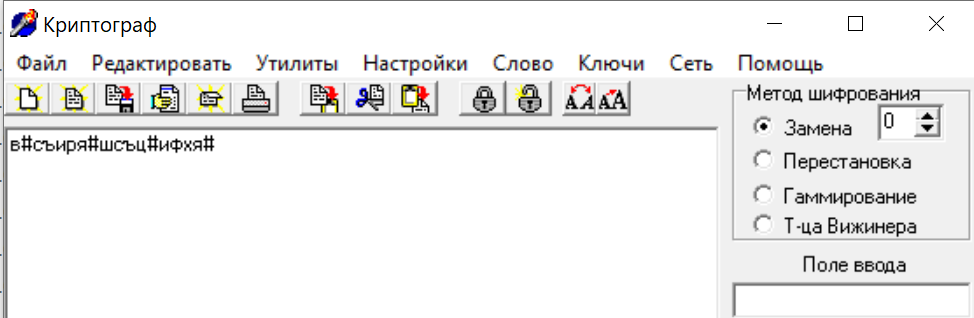


Рисунок 9 – Зашифрованный текст

По условию задания текст должен быть зашифрован со сдвигом от 3 до 9 символов. Вскрытие шифра происходит перебором вариантов. Были добавлены ключи 3-9 и была произведена дешифровка текста по этим ключам.

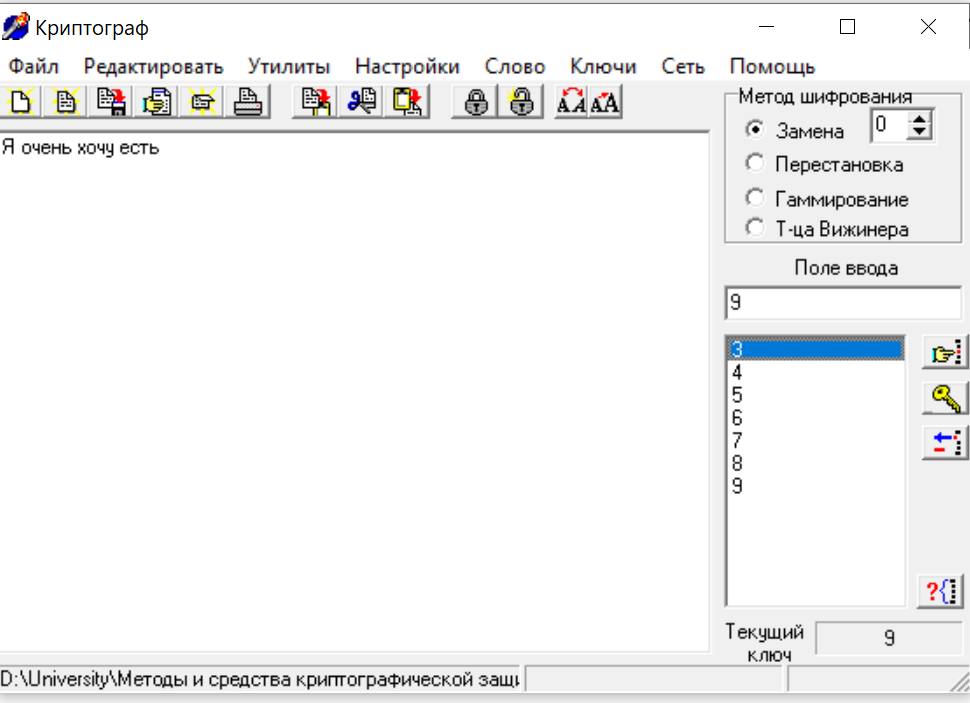


Рисунок 10 – Попытка 1, ключ3

Как видно из рисунка, при ключе 3 текст обретает смысл, следовательно 3 – ключ.

**На шаге номер 1 был найден верный сдвиг 3 символа**.

**Дешифрование перестановки**

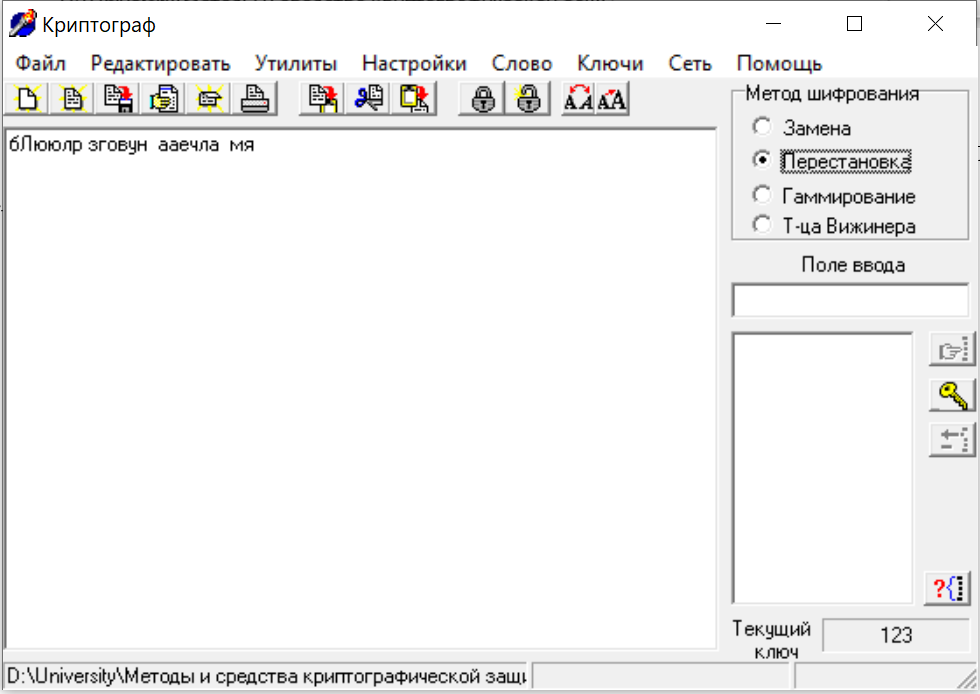


Рисунок 11 – Зашифрованный текст

Заметим, что в данном зашифрованном тексте присутствует заглавная буква, что вероятнее всего указывает на то, что она должна стоять в начале текста (то есть идет замена перестановка первого символа на второе место). Так же в первых 5 позициях есть повторяющееся две буквы Л и Ю, что наводит на мысль о слове «Люблю», которое было подвергнуто перестановке. Тогда существует 2 варианта ключа из 5 символов. Первый ключ 31254 и 31524.Проверим данные ключи.

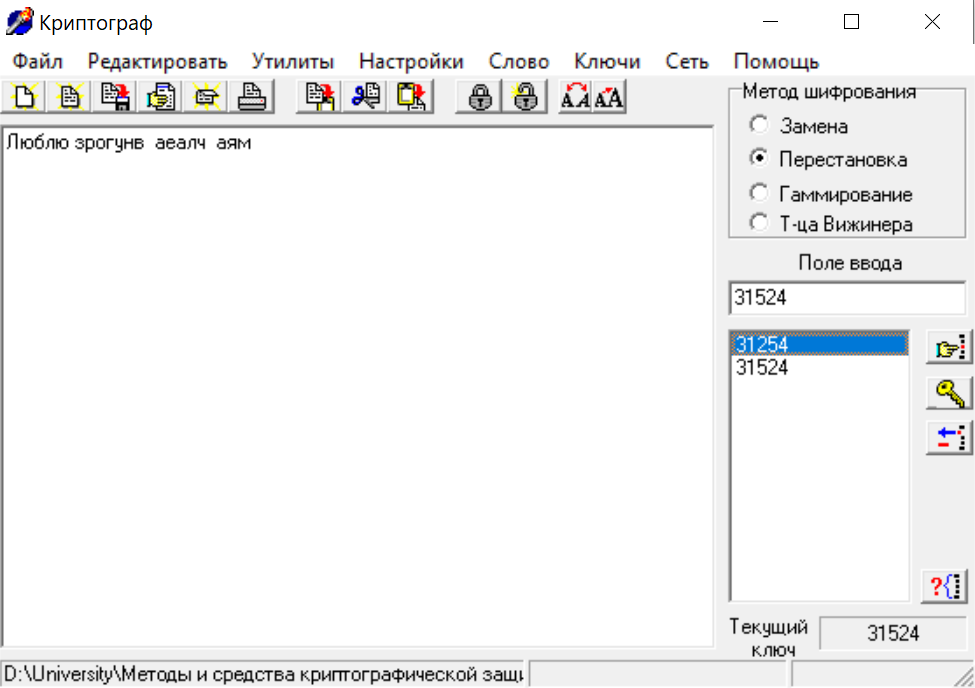


Рисунок 12 – Дешифровка ключ 31254

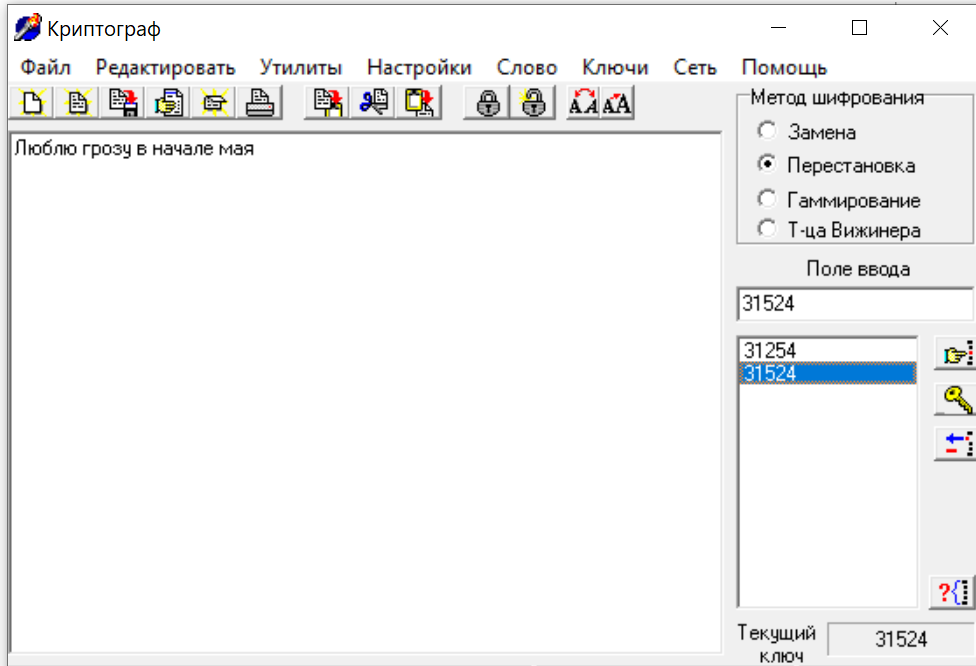


Рисунок 13 – Дешифровка ключ 31542

Из рисунков видно, что ключ 31524 является верным и позволяет дешифровать сообщение.

**На шаге номер 2 был найден верный ключ из 5 символов «31524»**.

**Дешифрование гаммирования**

Для дешифрования методом гаммирования необходимо сделать протяжку вероятного слова. Для протяжки вероятных слов были взяты самые часто встречающиеся слова в русском языке из 4 и 5 букв

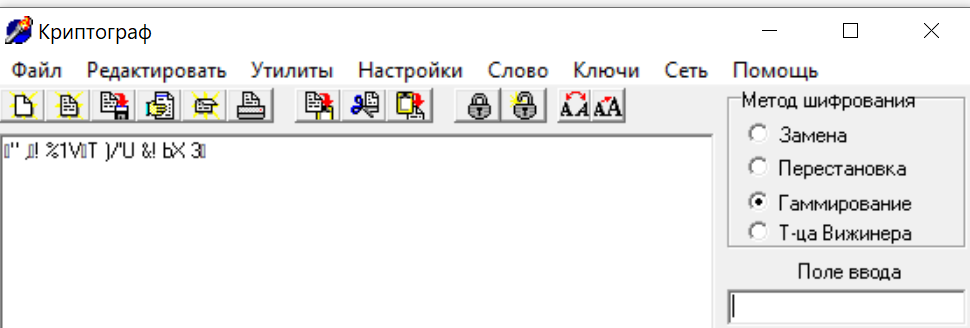


Рисунок 14 – Исходный текст

Шаг 1 протяжка вероятного слова «быть»

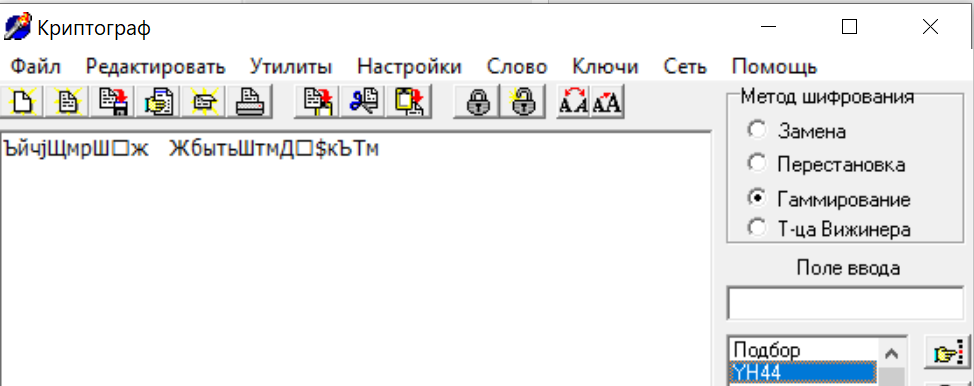


Рисунок 15 – Попытка дешифровки по ключевому слову «быть»

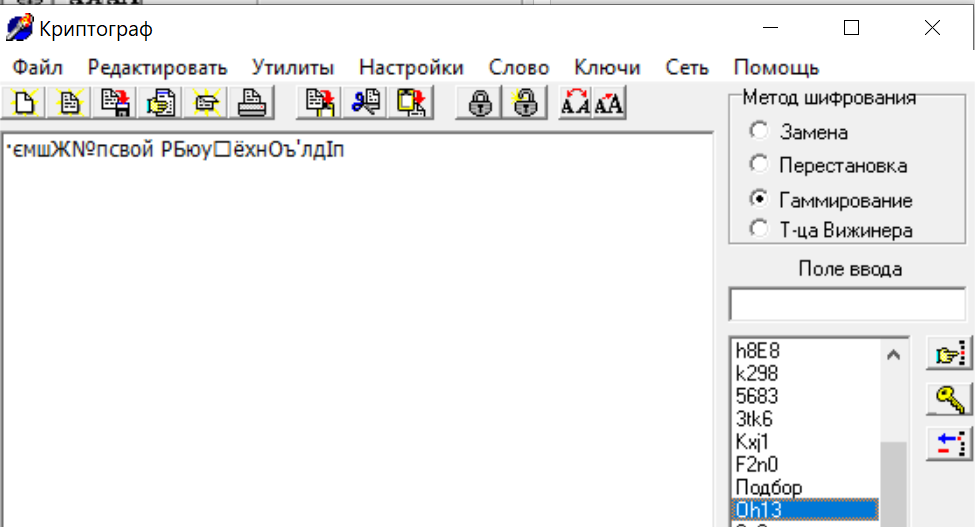


Рисунок 16 – Попытка дешифровки по ключевому слову «свой»

Заметим, что при таком ключе увеличилось количество символов кириллицы в тексте. Соответственно слово, которое встречается в тексте похоже на слово свой (имеет похожие буквы)

Попытка 153, протяжка слова «кони»

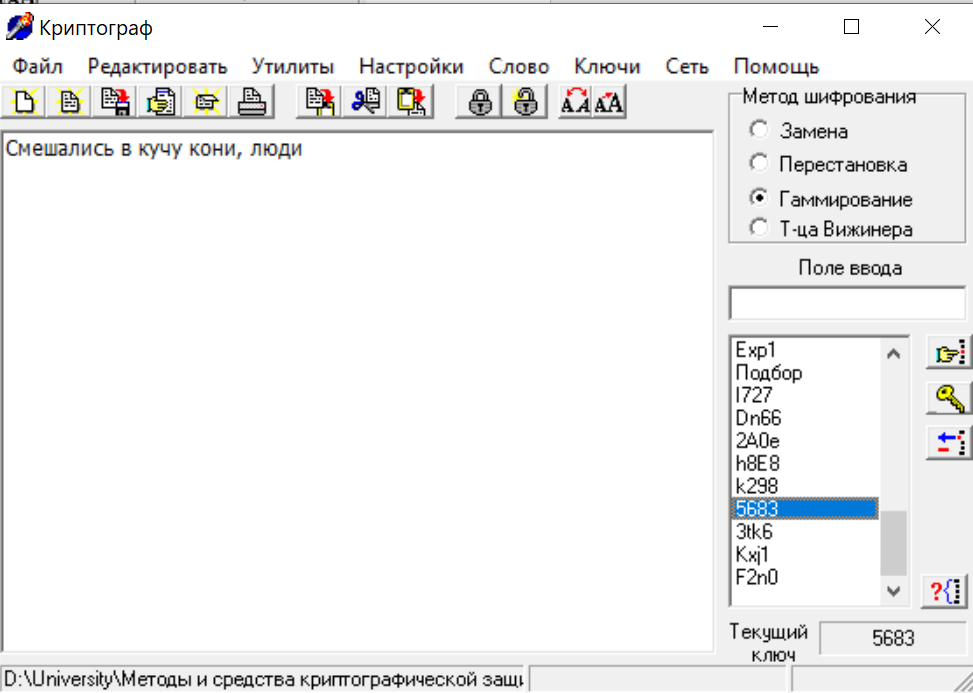


Рисунок 17 – Попытка дешифровки по ключевому слову «кони»

**На попытке 153 был найден ключ из 4 символов «5683»**

**Дешифрование таблицы Вижинера**

Для дешифрования текста, зашифрованного таблицей Вижинера будет использовать метод протяжки вероятного слова

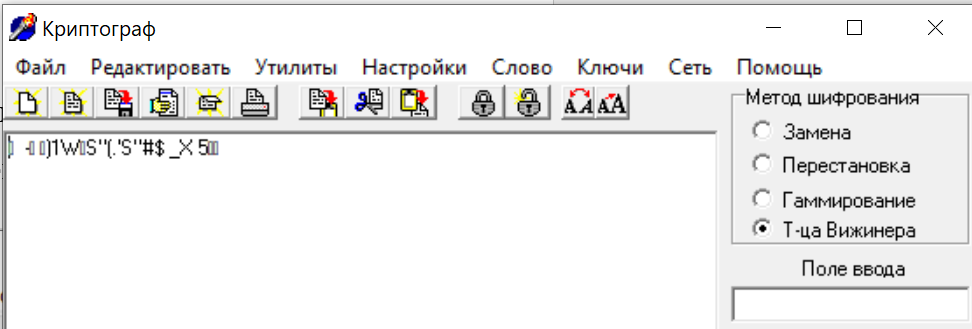
****

Рисунок 17 – Исходный текст

Протяжка первого вероятного слова «быть»

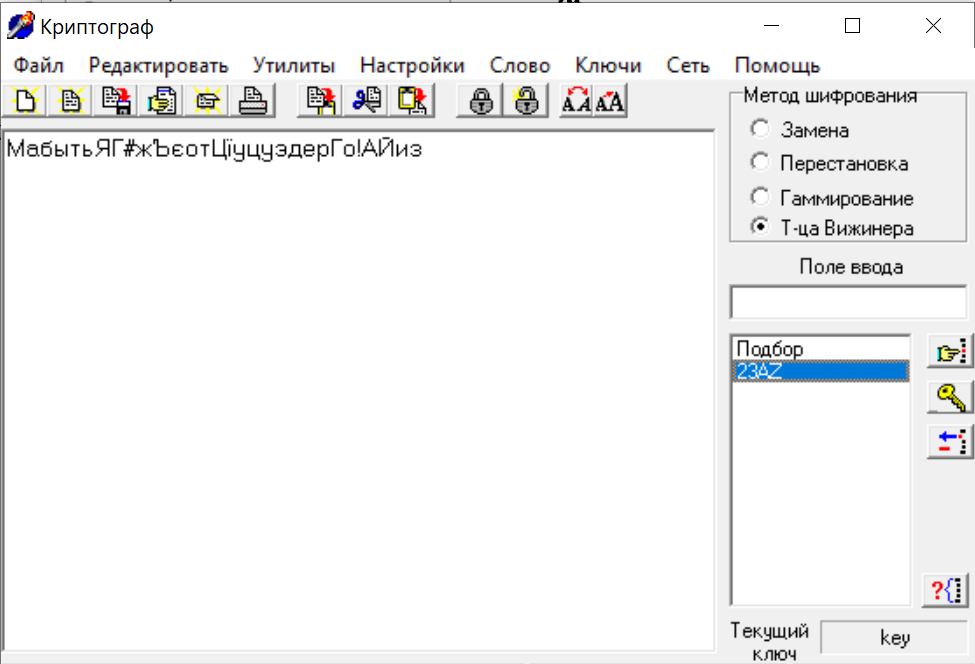


Рисунок 18 – Протяжка слова «быть»

На попытке 12 в качестве вероятного слова было выбрано слово вещи и в одном из возможных ключей появилось 2 осмысленных слова «Как» и «вещи». Это обозначает что реальный ключ крайне похож на найденный ключ «4385»

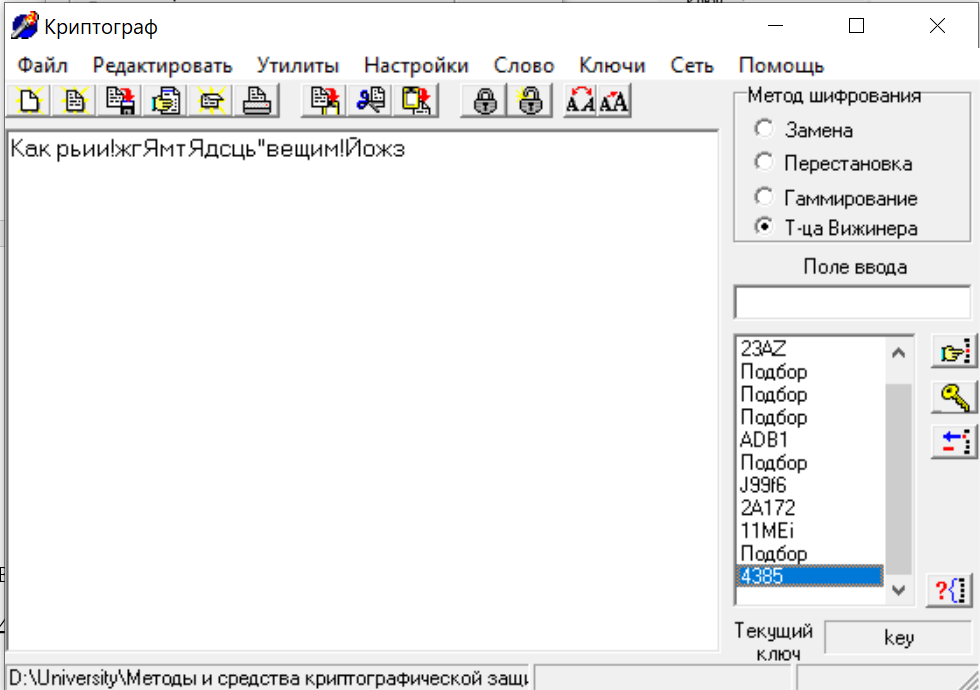


Рисунок 19 – Протяжка слова «вещи»

Путем подбора похожего слова было выбрано слова «вещий».

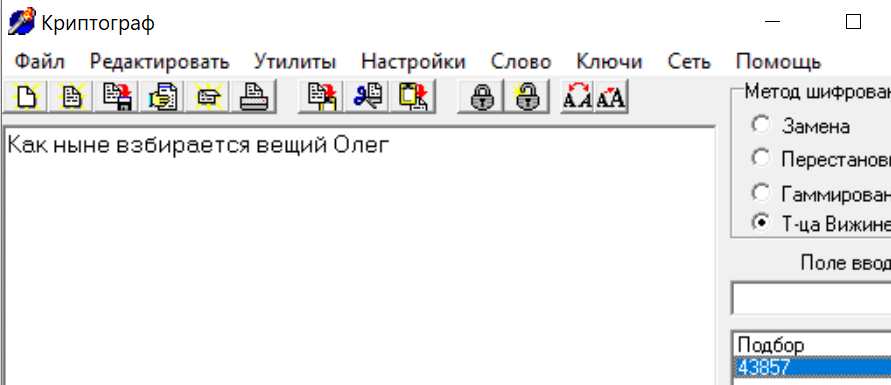


Рисунок 20 – Протяжка слова «вещий»

**На шаге 35 был найден ключ из 5 символов «43857»**