УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №1

по предмету «Теория информации»

Выполнил:

Захвей И.В.

гр. 351004

Проверила:

Болтак С.В.

Минск 2025

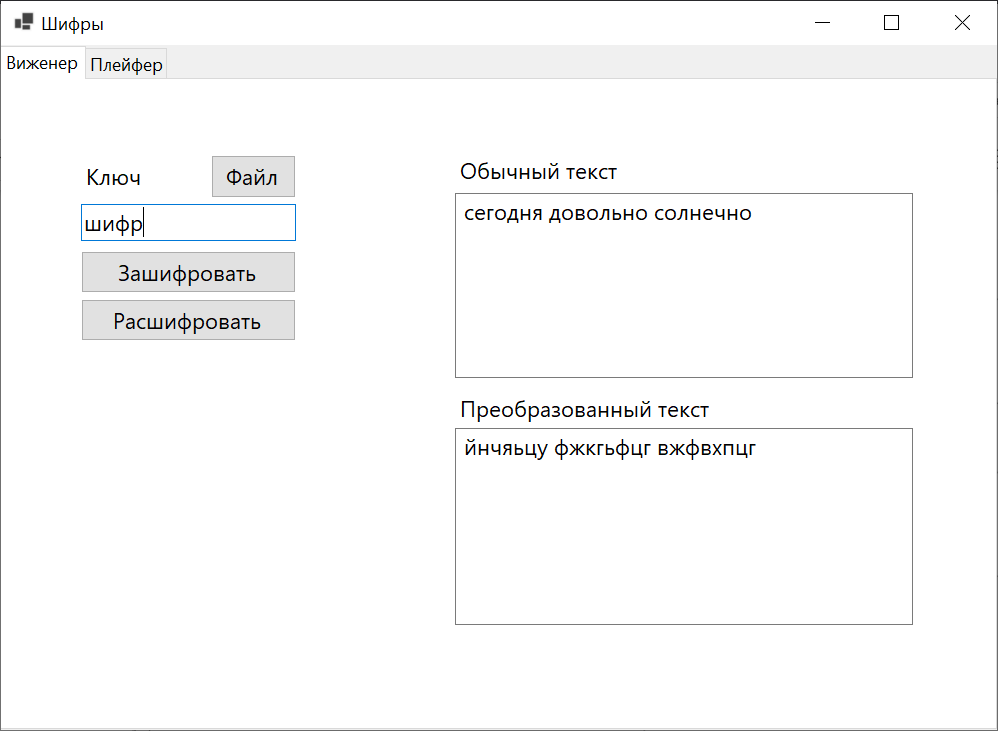
Вариант №11.

**Шифр Виженера**

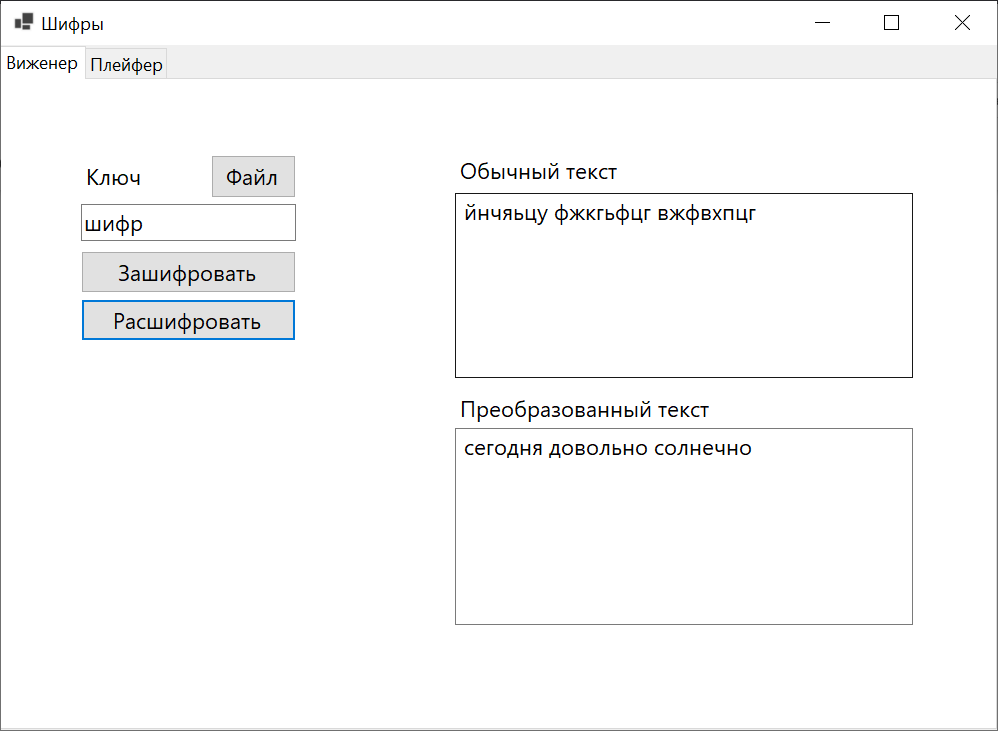
1.Тестовая фраза: “сегодня довольно солнечно”;

Ключ “шифр”;

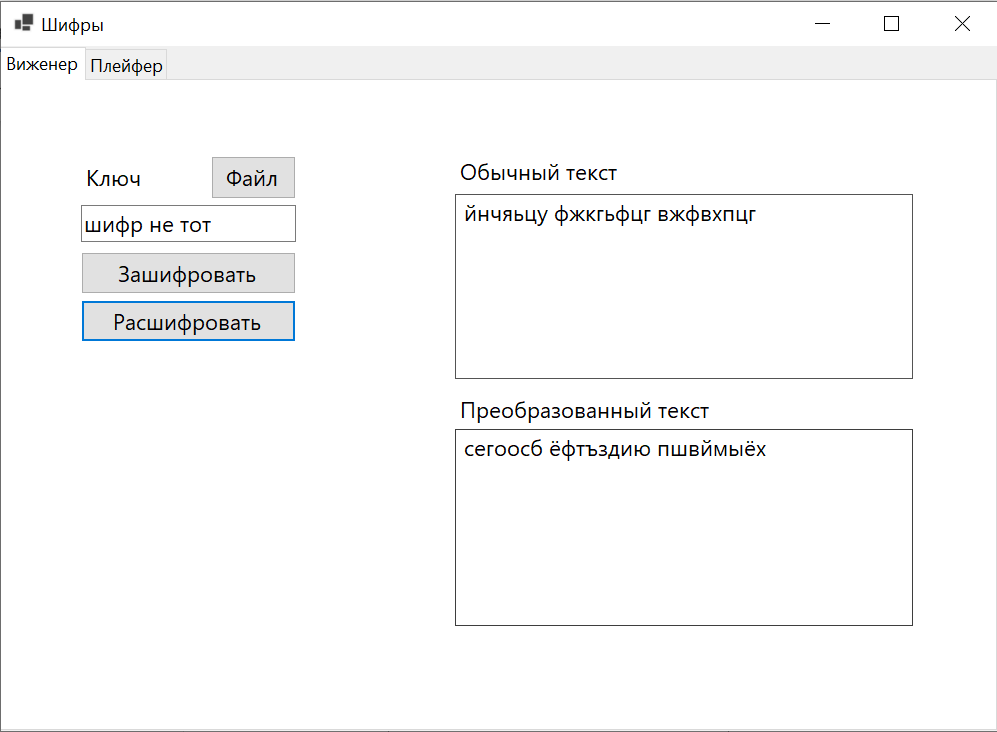
Шифротекст: “йнчяьцу фжкгьфцг вжфвхпцг”



Если ключ тот же то данные нормальные.



Вывод, если шифр не тот:

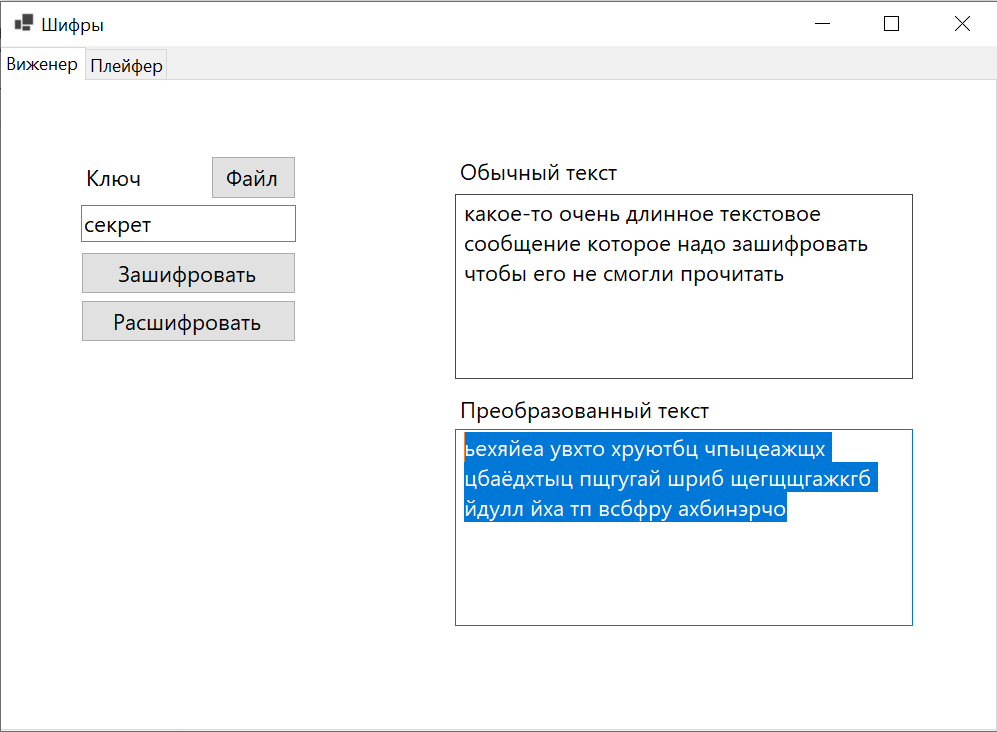


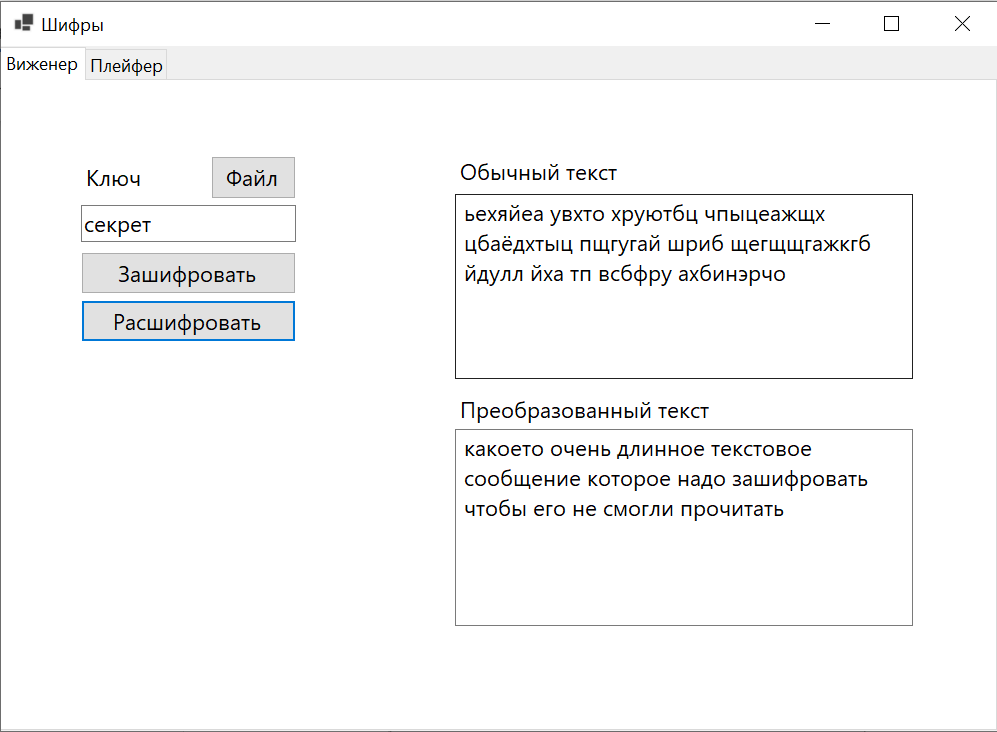
**ТЕСТ ПРОЙДЕН**

Тестовая фраза: “какое-то очень длинное текстовое сообщение которое надо зашифровать чтобы его не смогли прочитать”;

Ключ “секрет”;

Шифротекст: ” ьехяйеа увхто хруютбц чпыцеажщх цбаёдхтыц пщгугай шриб щегщщгажкгб йдулл йха тп всбфру ахбинэрчо”



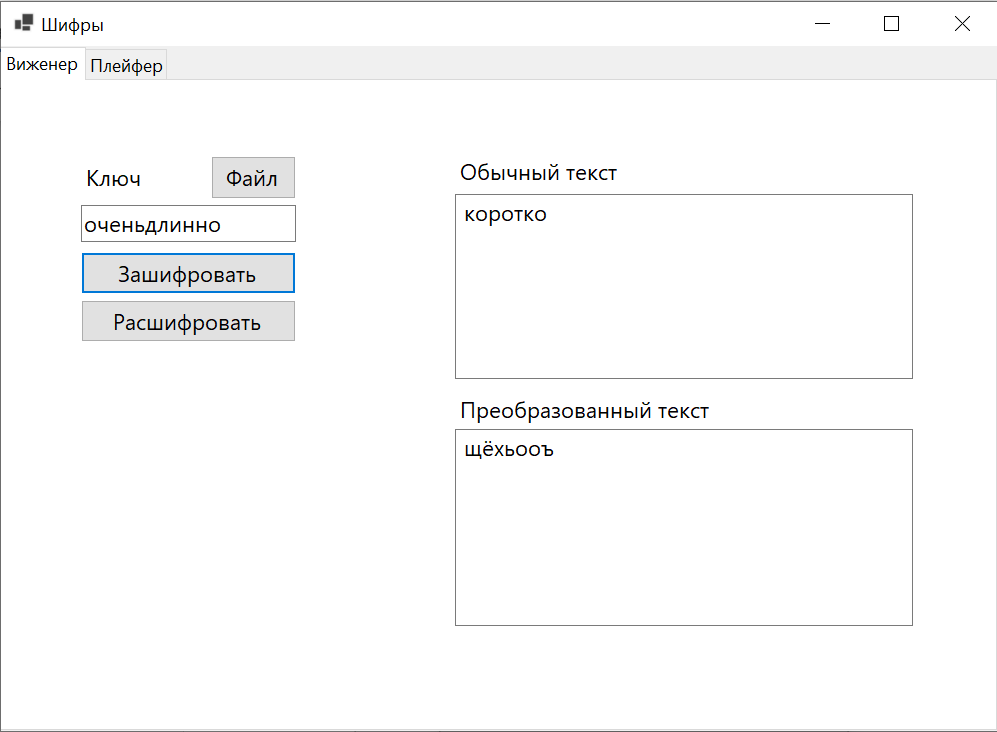


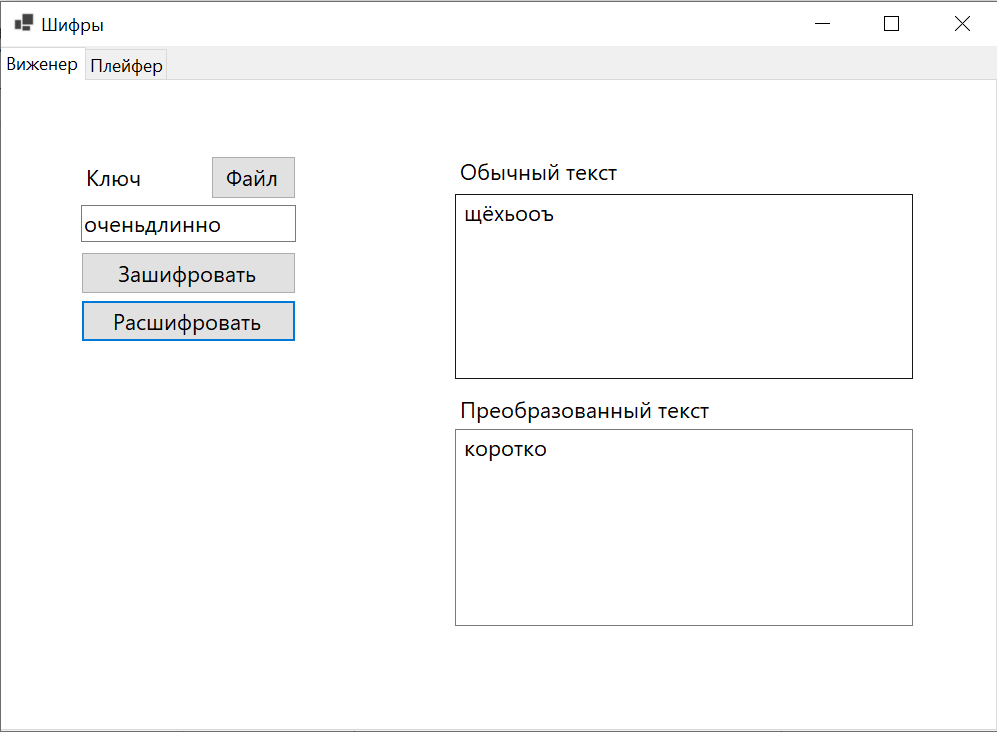
**ТЕСТ ПРОЙДЕН**

3. Ключ больше исходного:

Тестовая фраза: “коротко”;

Ключ “оченьдлинно”;

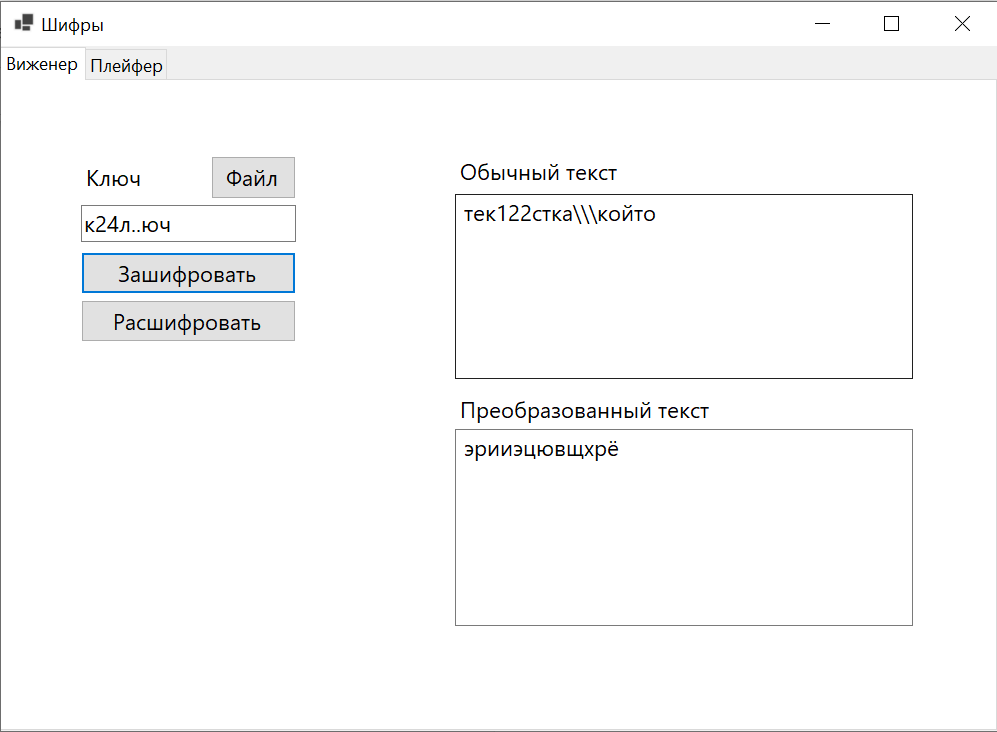


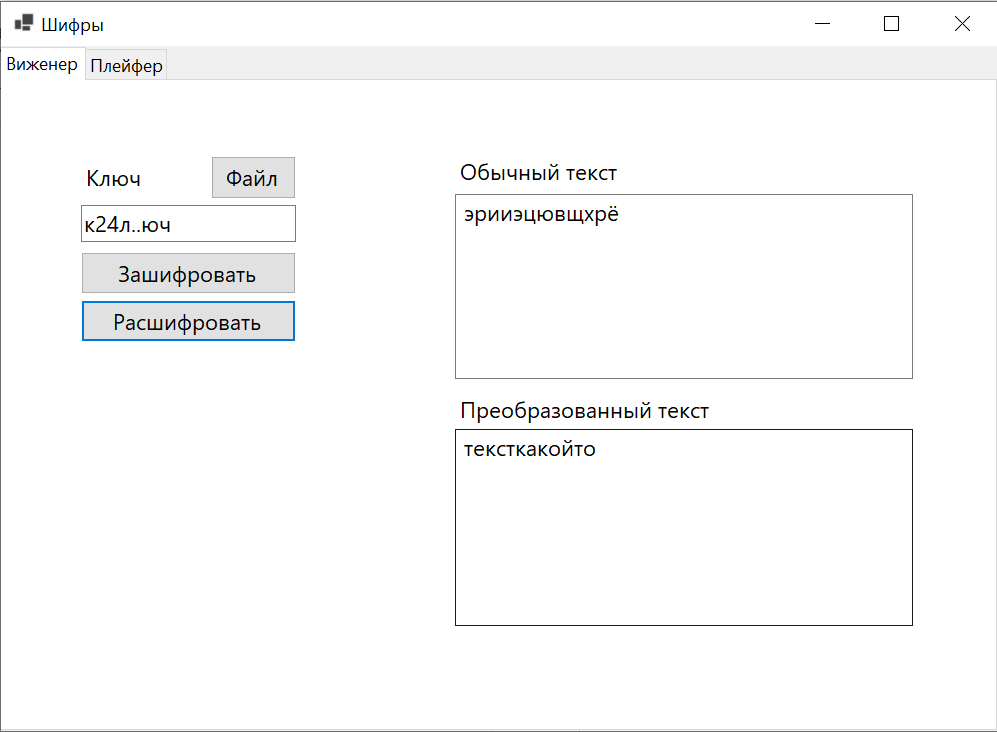


**ТЕСТ ПРОЙДЕН**

4. Недопустимые значения:

Тестовая фраза: тексткакойто;





**ТЕСТ ПРОЙДЕН**

**Шифр Плейфера с 4мя матрицами**

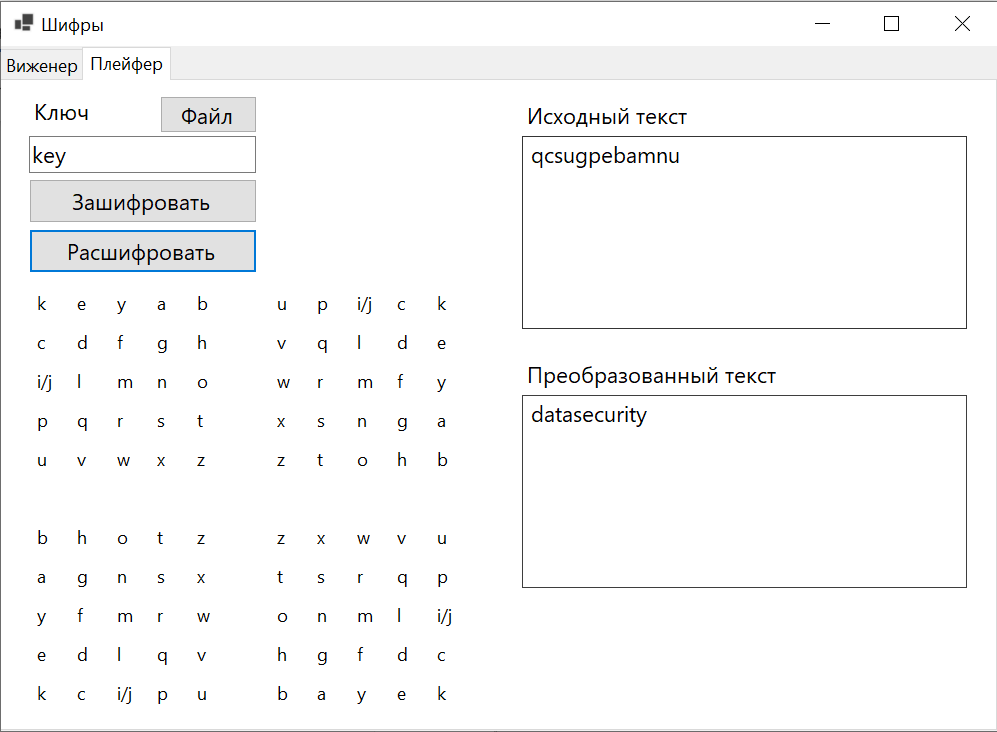
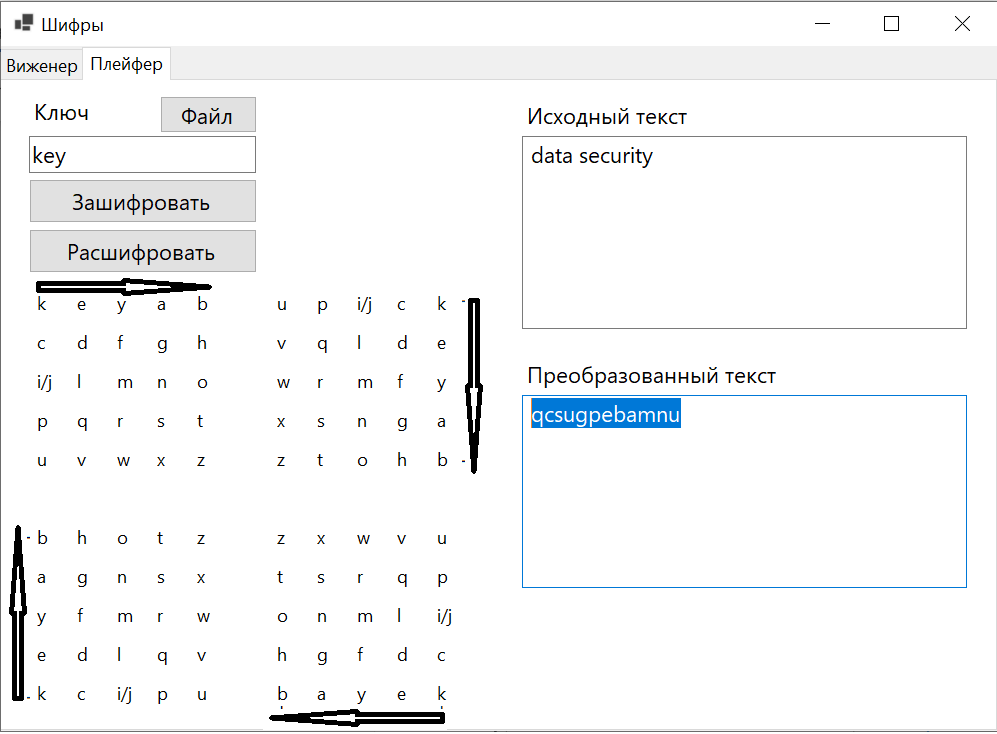
1. *Дымовое тестирование:*

Тестовая фраза: “data security”;

Ключ “key”;

Шифротекст: " qcsugpebamnu”

На картинке я попытался указать как строю 4 матрицы. Так как я не нашел инструкций как строить эти матрицы, а на лекции сказали, что это зависит от реализации, я решил использовать метод, который используется в обычном шифровании Плейфера для первой подматрицы, а остальные получать поворотом исходной на 90 градусов. Стрелки показывают как идет изначальная первая строка первой матрицы. Таким образом ключ можно задать одним словом.



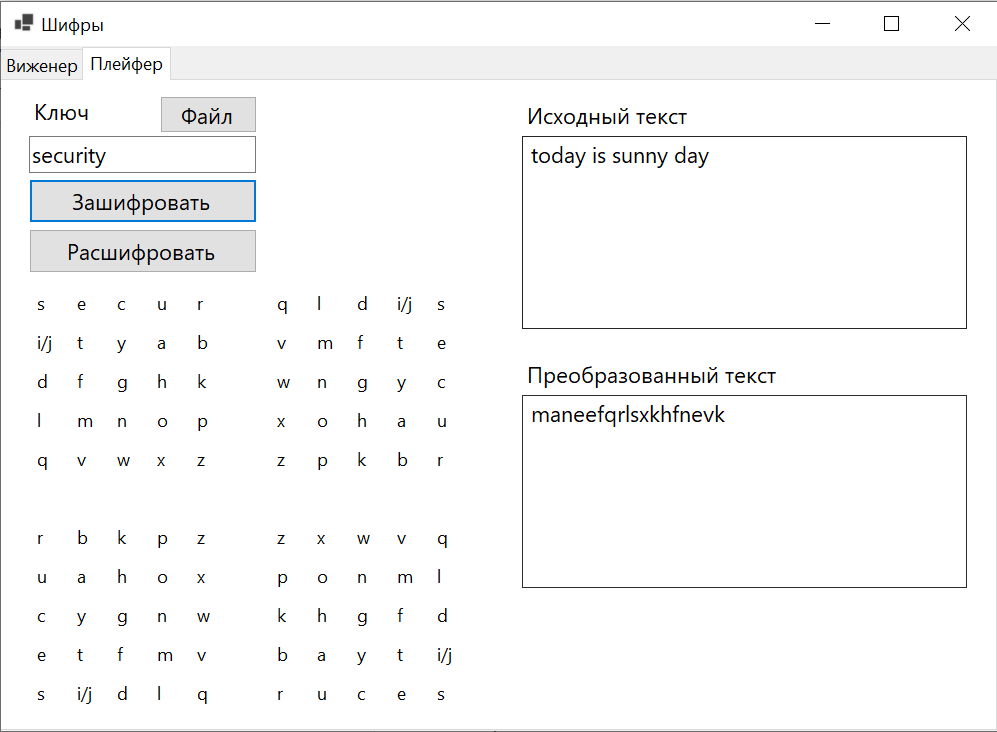
**ТЕСТ ПРОЙДЕН**

1. Другой ключ (матрица поменялась):

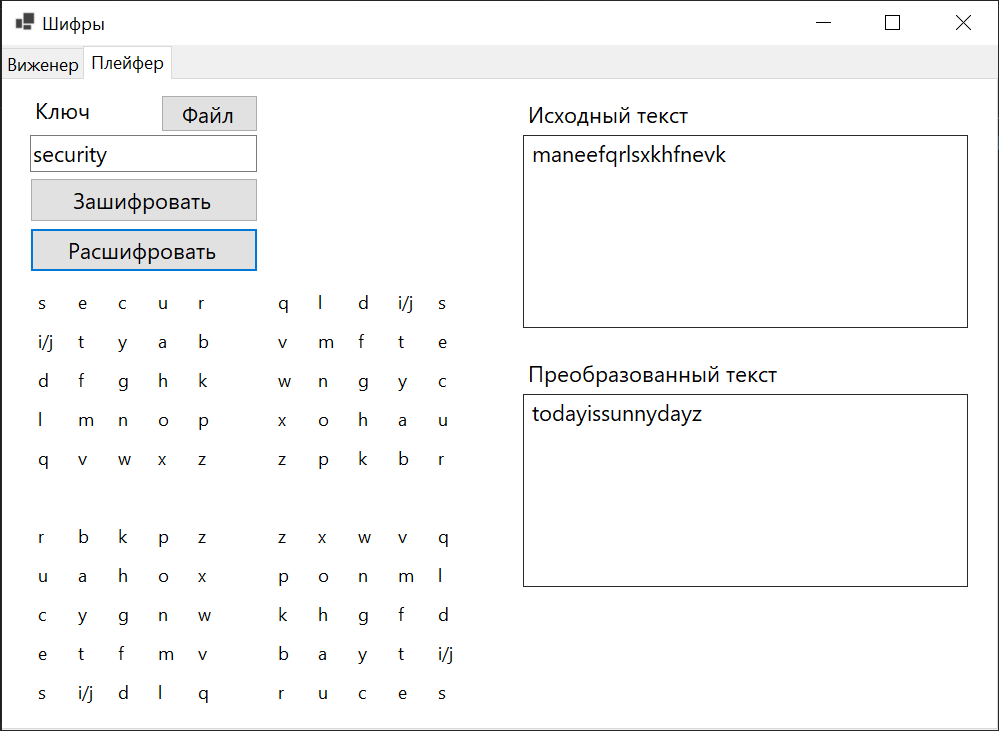
Тестовая фраза: today is sunny day;

Ключ: security;

Шифротекст: maneefqrlsxkhfnevk



Расшифрованный текст содержит в себе буквы “z” это разделители, те что должны находится между одинаковыми символами программа удаляет при расшифровке, а “z”, который подставляется в конце программно удалить не представляется возможным, т.к. зависит от смысла.



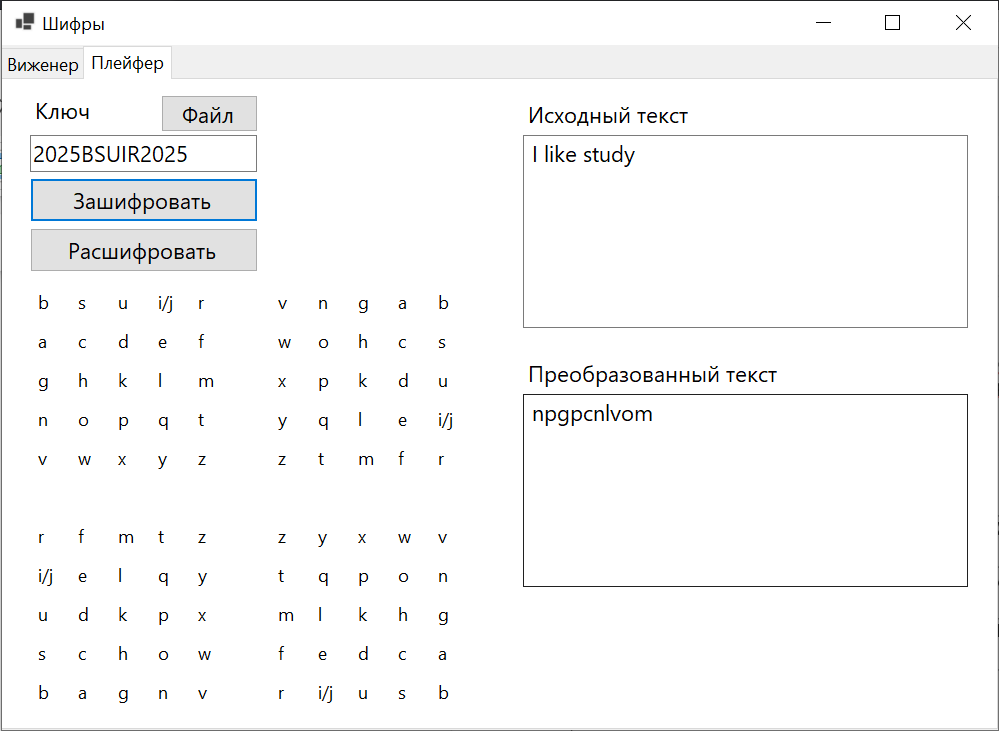
**ТЕСТ ПРОЙДЕН**

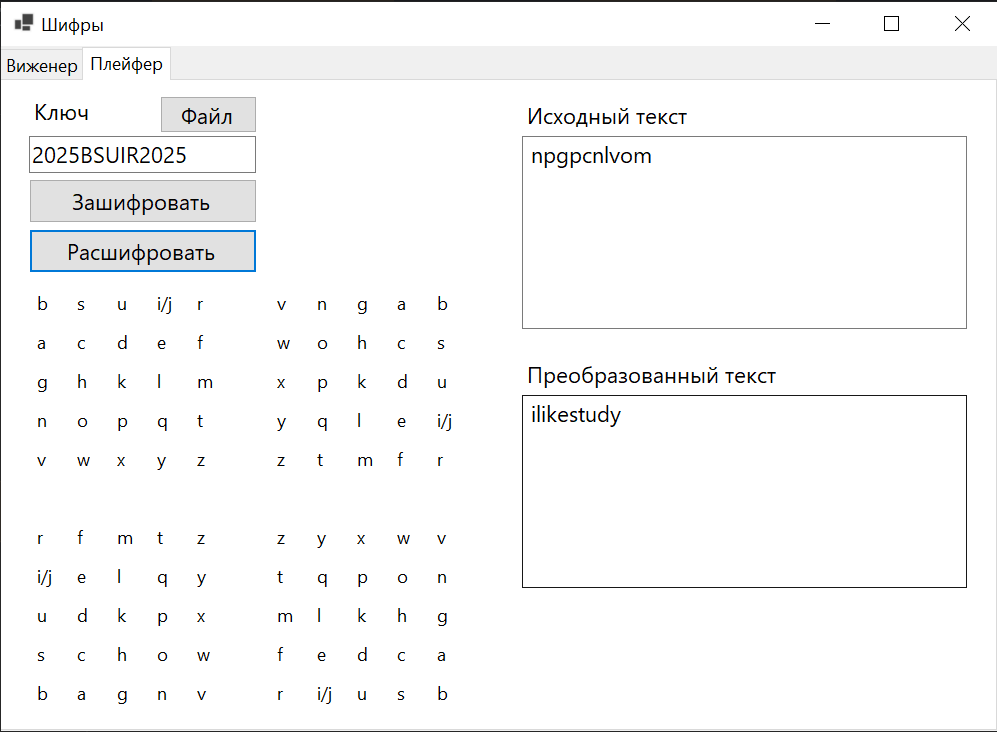
1. Ввод ключа с недопустимыми символами

Тестовая фраза: i like study;

Ключ 2025BSUIR2025;

Шифротекст: npgpcnlvom

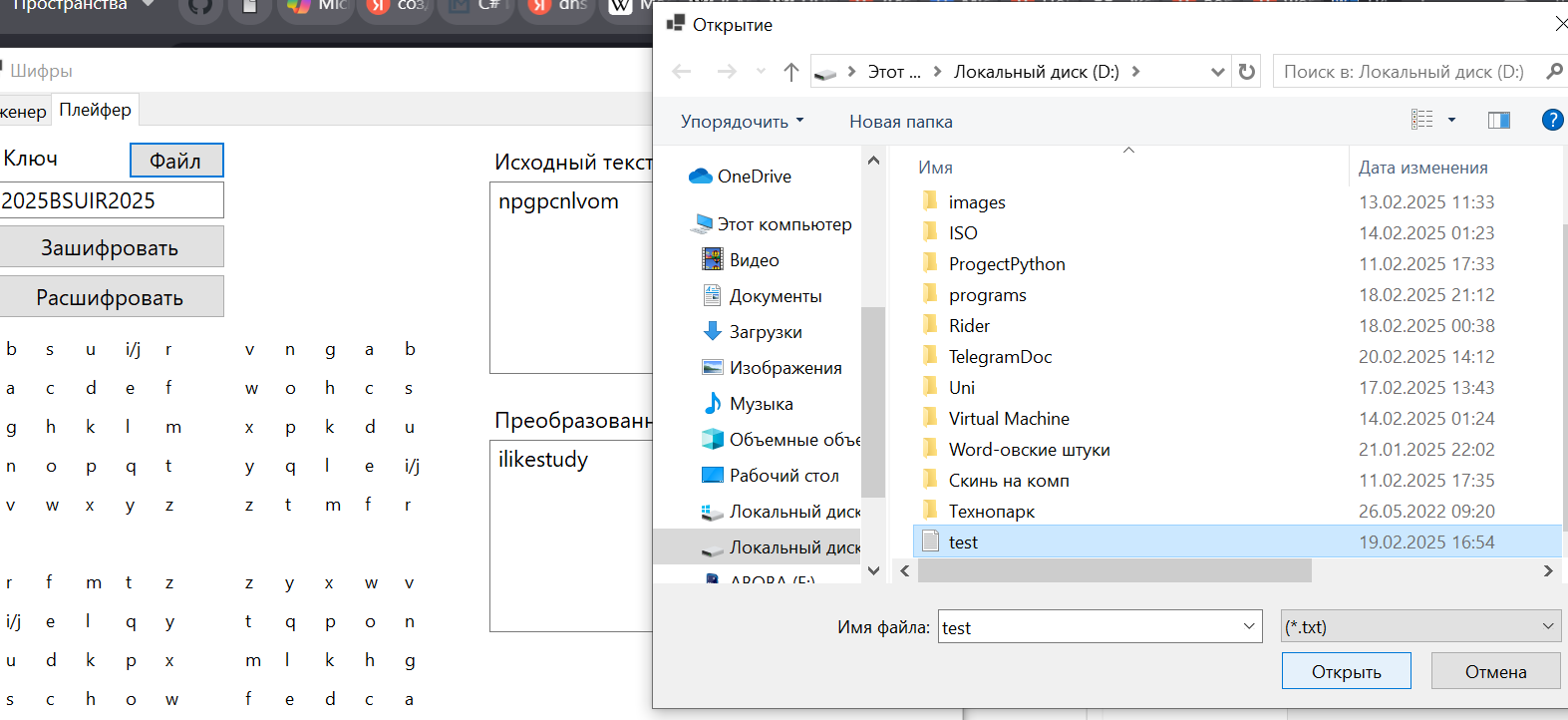




**ТЕСТ ПРОЙДЕН**

**СКРИНШЕТЫ РАБОТЫ**

**Работа выбора файлов**



**Уведомление о пустых полях**

