**Липецкий государственный технический университет**

Университетский колледж

Кафедра автоматизированных систем управления

Лабораторная работа №4

по «Защита информации»

Алгоритм шифрования DES

Студент Щеглов Д.A

Группа T-ИС-20

Руководитель Седых Ю.И

Липецк 2022г.

Оглавление

[Цель работы 3](#_Toc96780512)

[Алгоритм шифрования DES 4](#_Toc96780513)

# **Цель работы**

Изучить принцип работы симметричных алгоритмов шифрования на

примере алгоритма DES.

# **Алгоритм шифрования DES**

DES — блочный алгоритм, то есть при шифровании исходное сообщение переводится в двоичный код, а затем разбивается на блоки и каждый блок отдельно зашифровывается (расшифровывается). По стандарту (принят в 1977 году) размер блока DES равен 64 бита, то есть используя 8-ми битовую кодировку ASCII, применяемую в те времена, получим в одном блоке — 8 символов.

Основные достоинства алгоритма DES:

* используется только один ключ длиной 56 битов;
* зашифровав сообщение с помощью одного пакета, для расшифровки вы можете использовать любой другой;
* относительная простота алгоритма обеспечивает высокую скорость обработки информации;
* достаточно высокая стойкость алгоритма.

DES осуществляет шифрование 64-битовых блоков данных с помощью 56-битового ключа. Расшифрование в DES является операцией обратной шифрованию и выполняется путем повторения операций шифрования в обратной последовательности (несмотря на кажущуюся очевидность, так делается далеко не всегда.

Шифрование слово происходит через файл. Для начала нужно создать текстовый документ с тем что мы хотим зашифровать. Далее в программе указать ключ равный 8 символам.

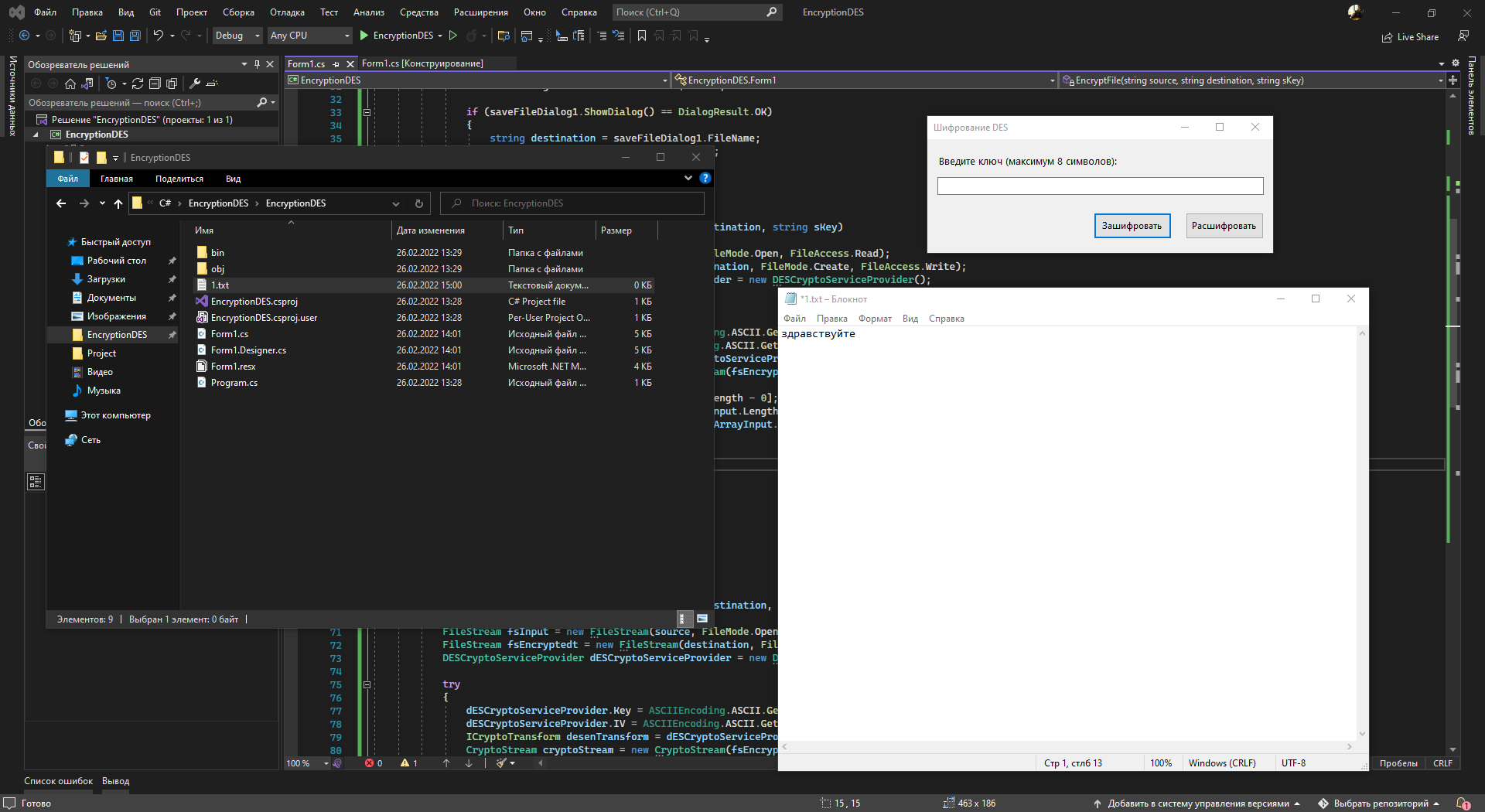


Рисунок 1.

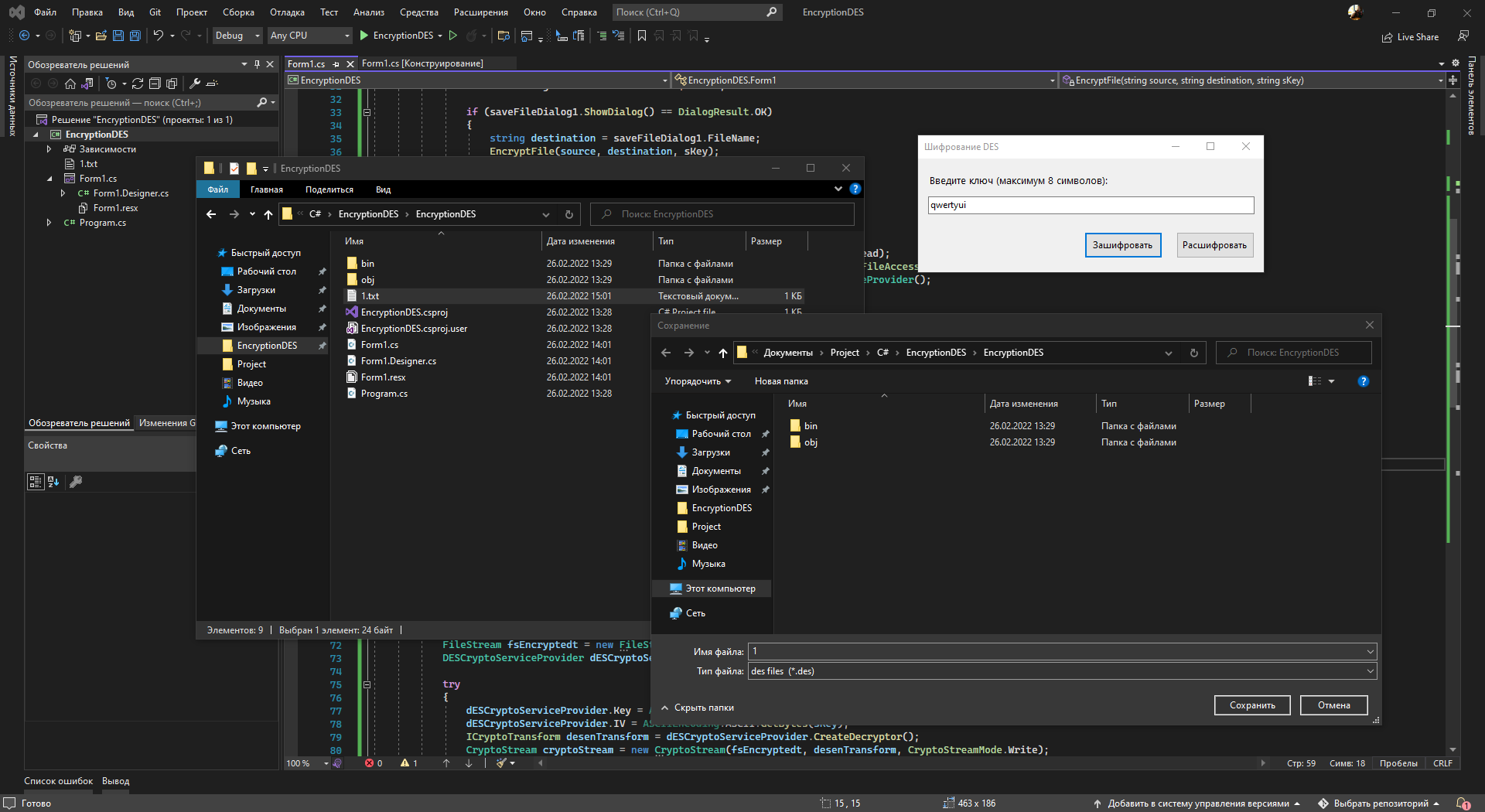


Рисунок 2.

Указываем ключ, в моём случае «qwertyui» и жмём на кнопку «Зашифровать», у нас открывается диалоговое окно с открытием TXT и cохранением .des файла

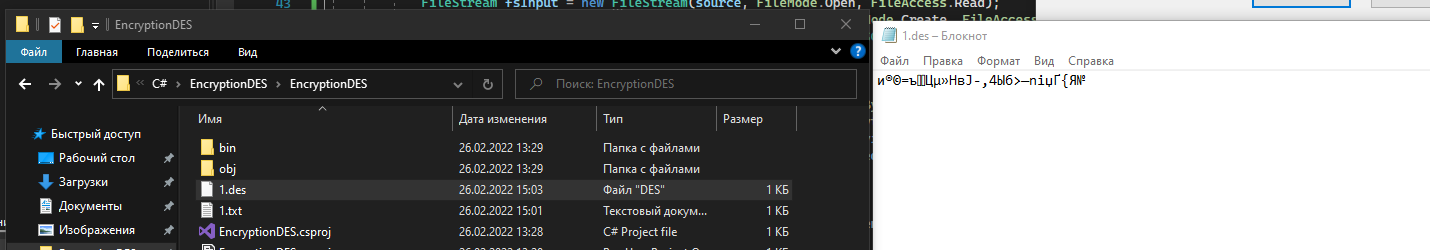


Рисунок 3.

На рисунке 3 показан зашифрованный файл

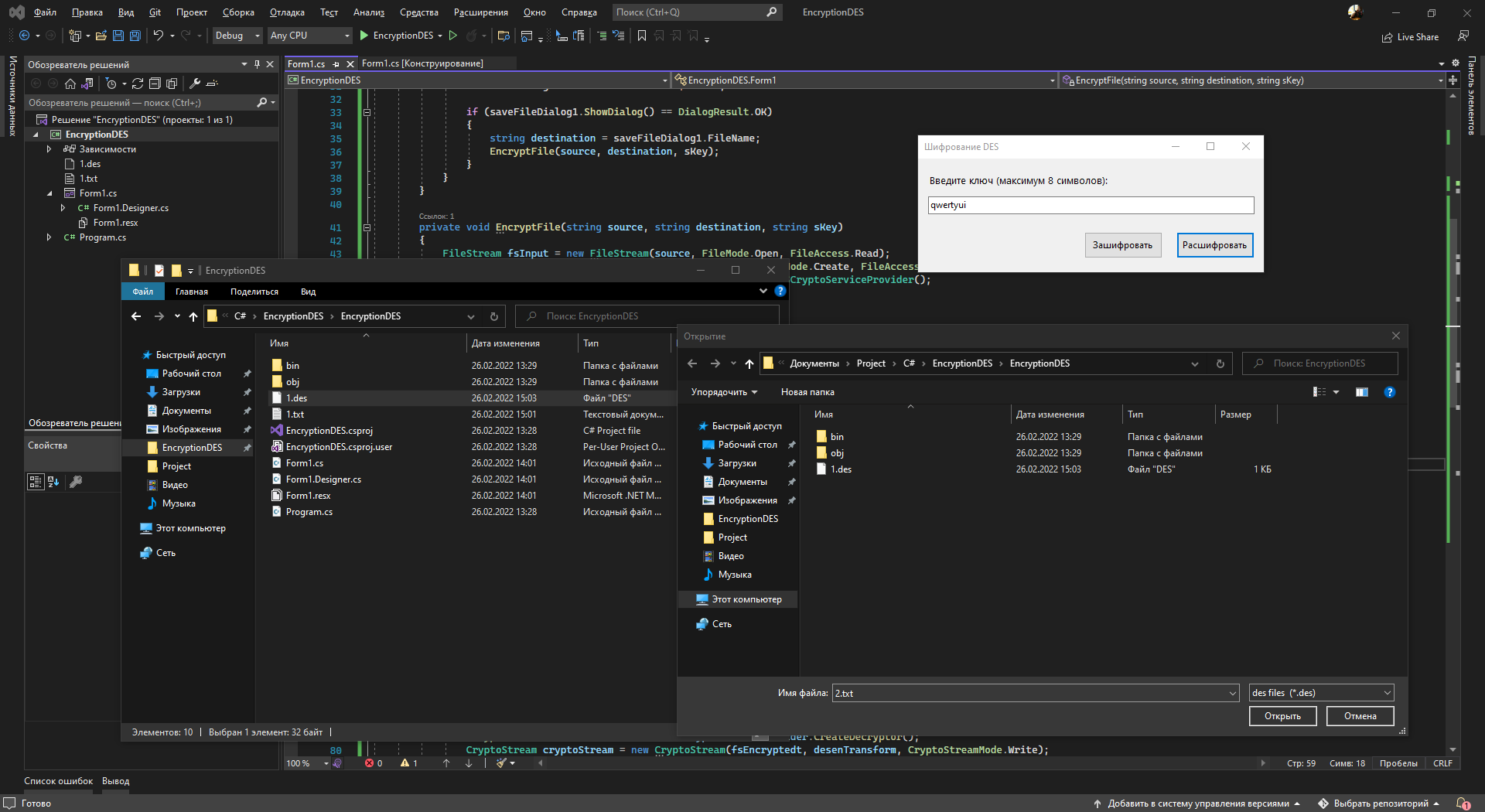


Рисунок 4.

На рисунке 4 произведена расшифровка файла и сохранение его в папку с проектом.

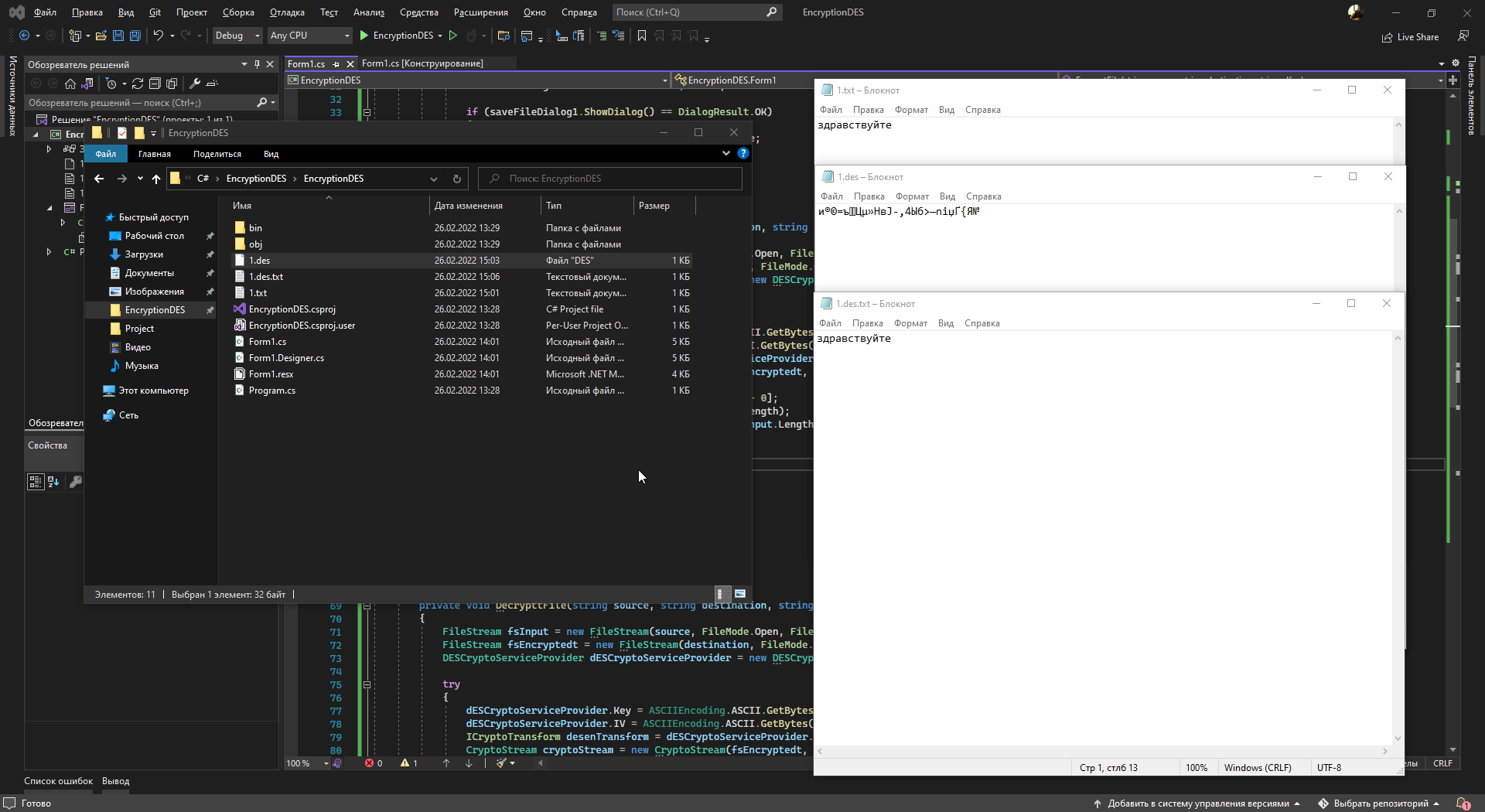


Рисунок 5.