УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №2 по предмету

Теория информации

Вариант 14

Выполнила:

Лутай В.В.

Проверила:

Болтак С.В.

Группа:

351003

Минск 2025

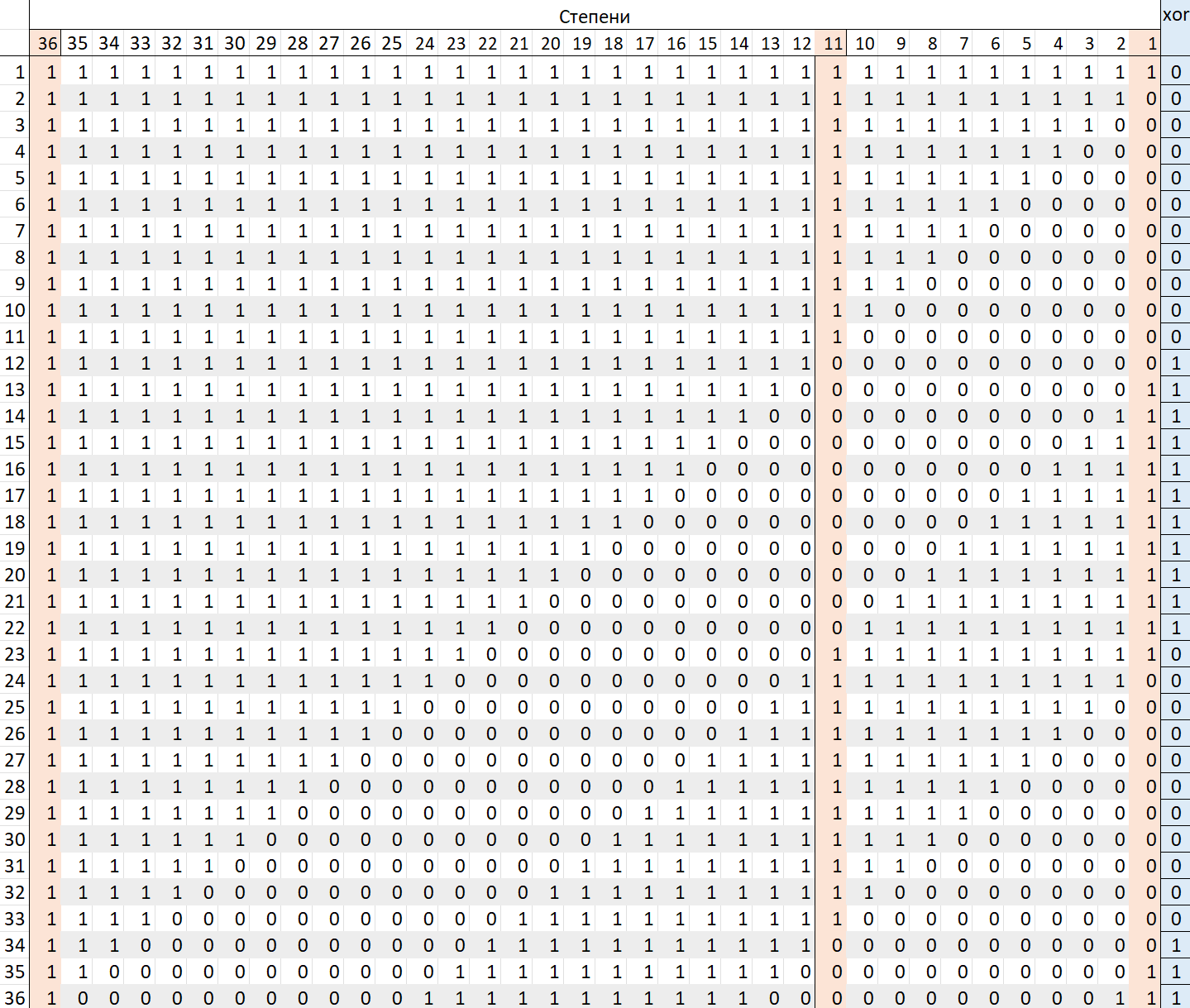
**Задания для варианта**

Реализовать систему потокового шифрования и дешифрования для файла с любым содержимым с помощью генератора ключевой последовательности на основе линейного сдвигового регистра с обратной связью LFSR1 (размерность регистра приведена в таблице №1). Начальное состояние регистра ввести с клавиатуры. Поле для ввода состояния регистра должно игнорировать любые символы кроме 0 и 1. Вывести на экран сгенерированный ключ (последовательность из 0 и 1), исходный файл и зашифрованный файл в двоичном виде. Программа не должна быть написана в консольном режиме. Результат работы программы – зашифрованный/расшифрованный файл.

**Многочлен для 14 варианта:**

*x*36 + *x*11 + 1

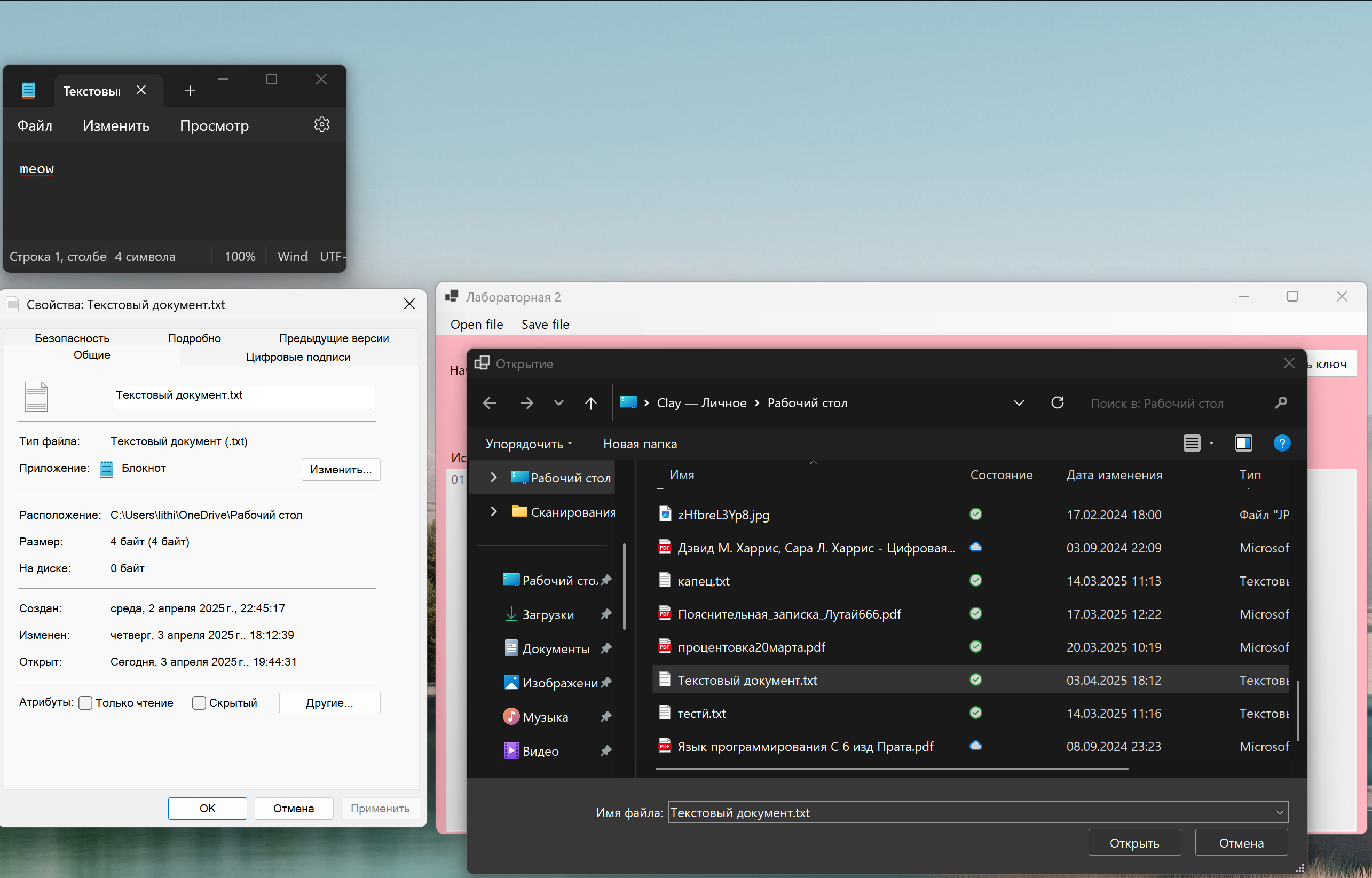
**Таблица:**



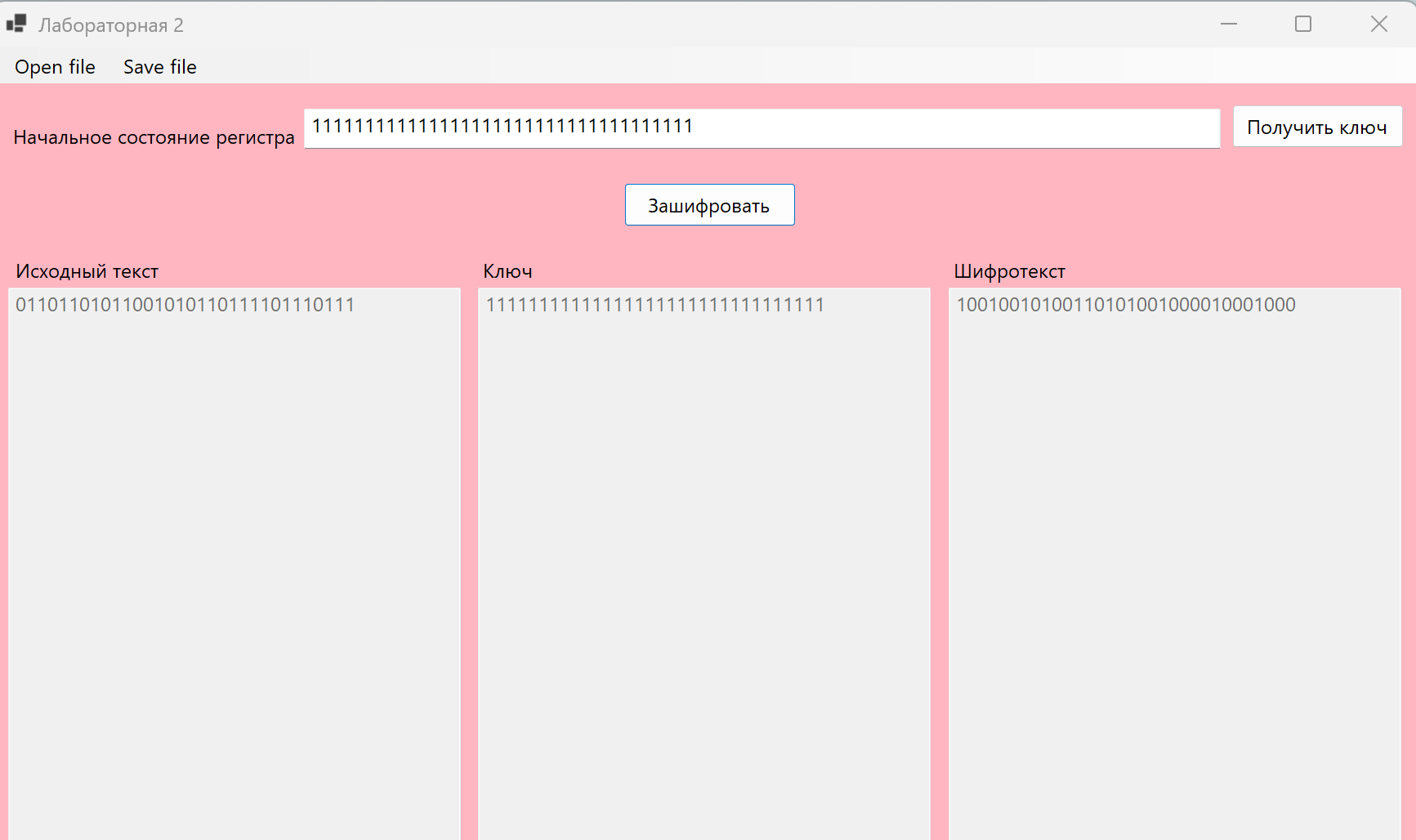


**Скриншоты:**

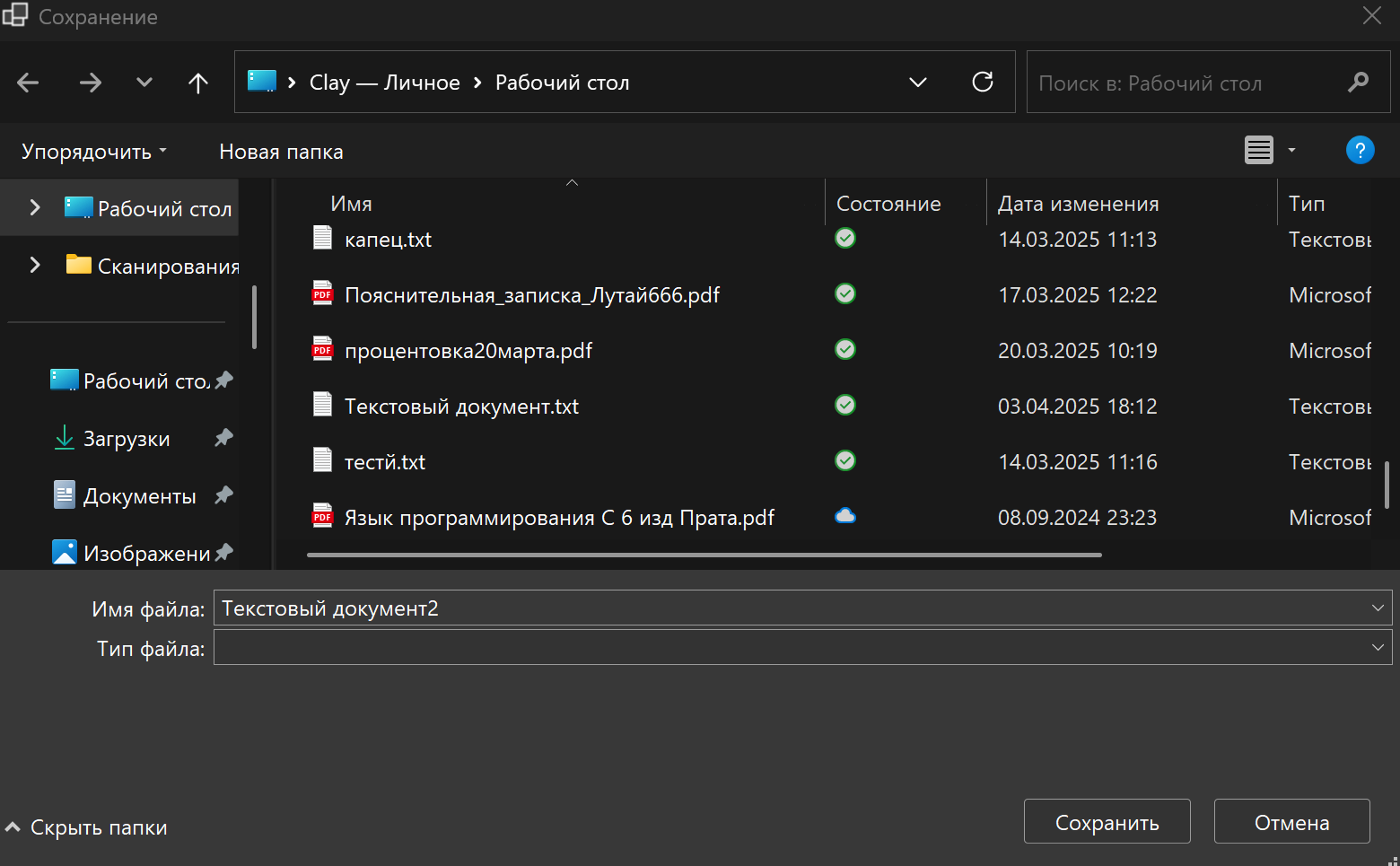
Текстовый файл:



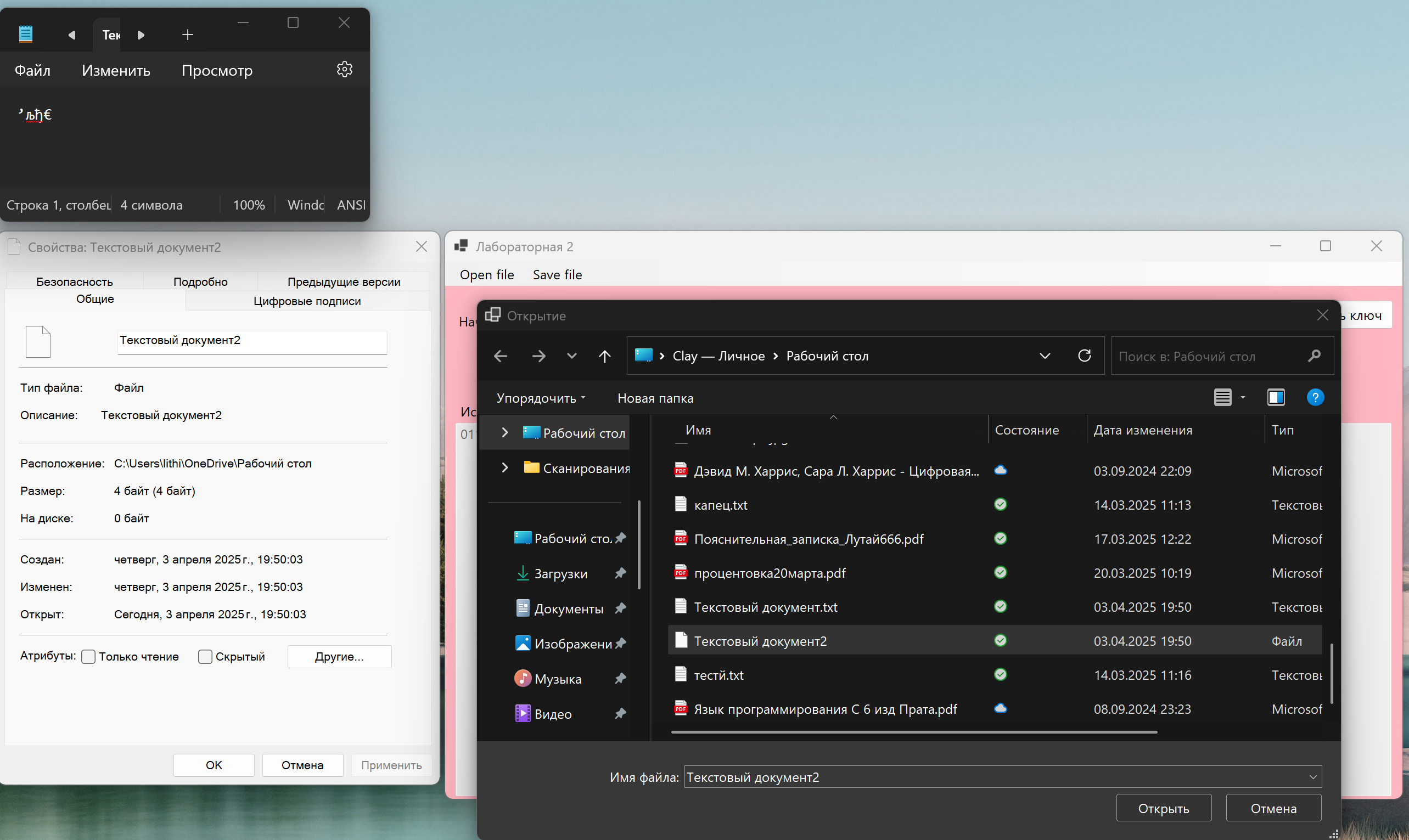
Шифрование:



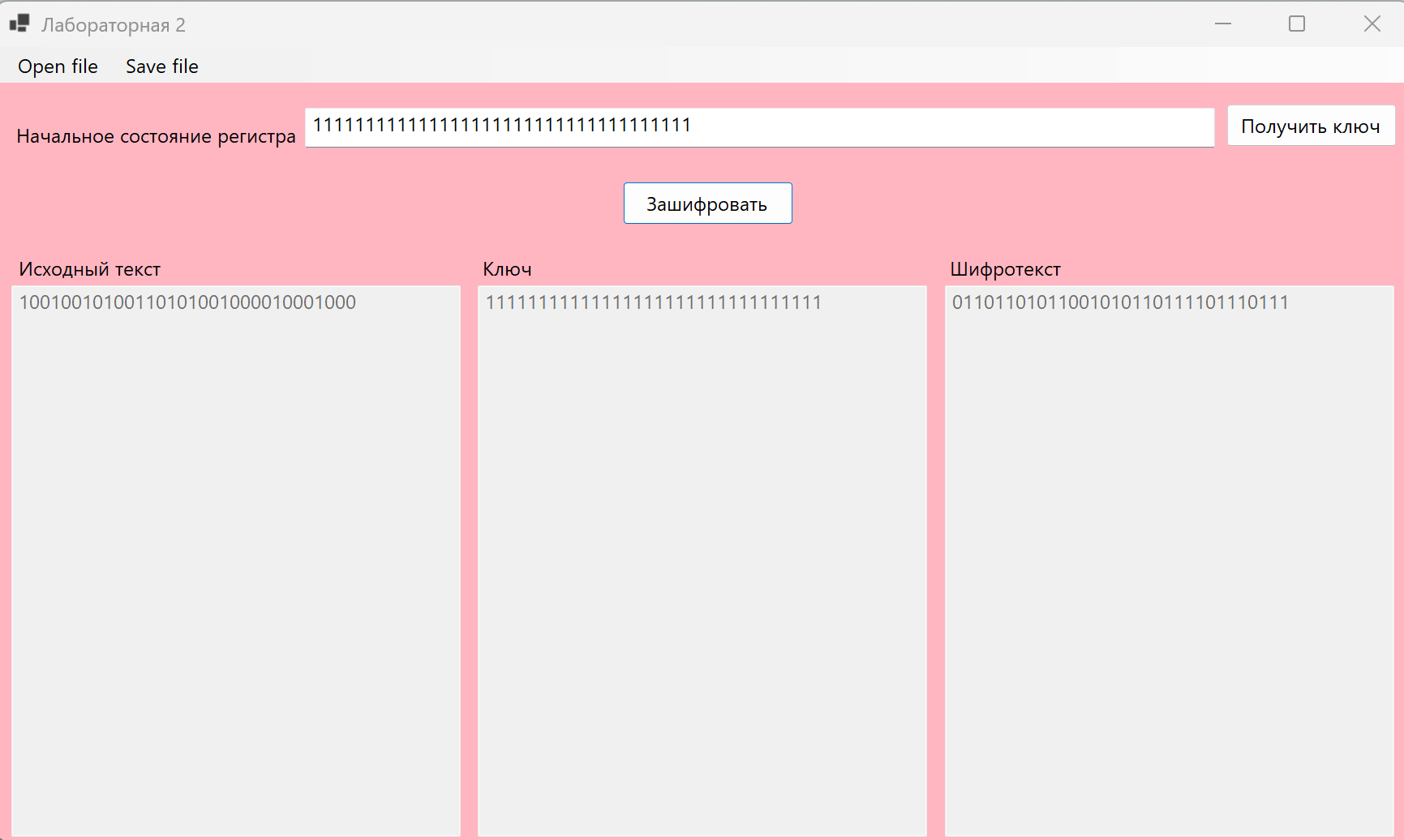
Сохранение в файл:



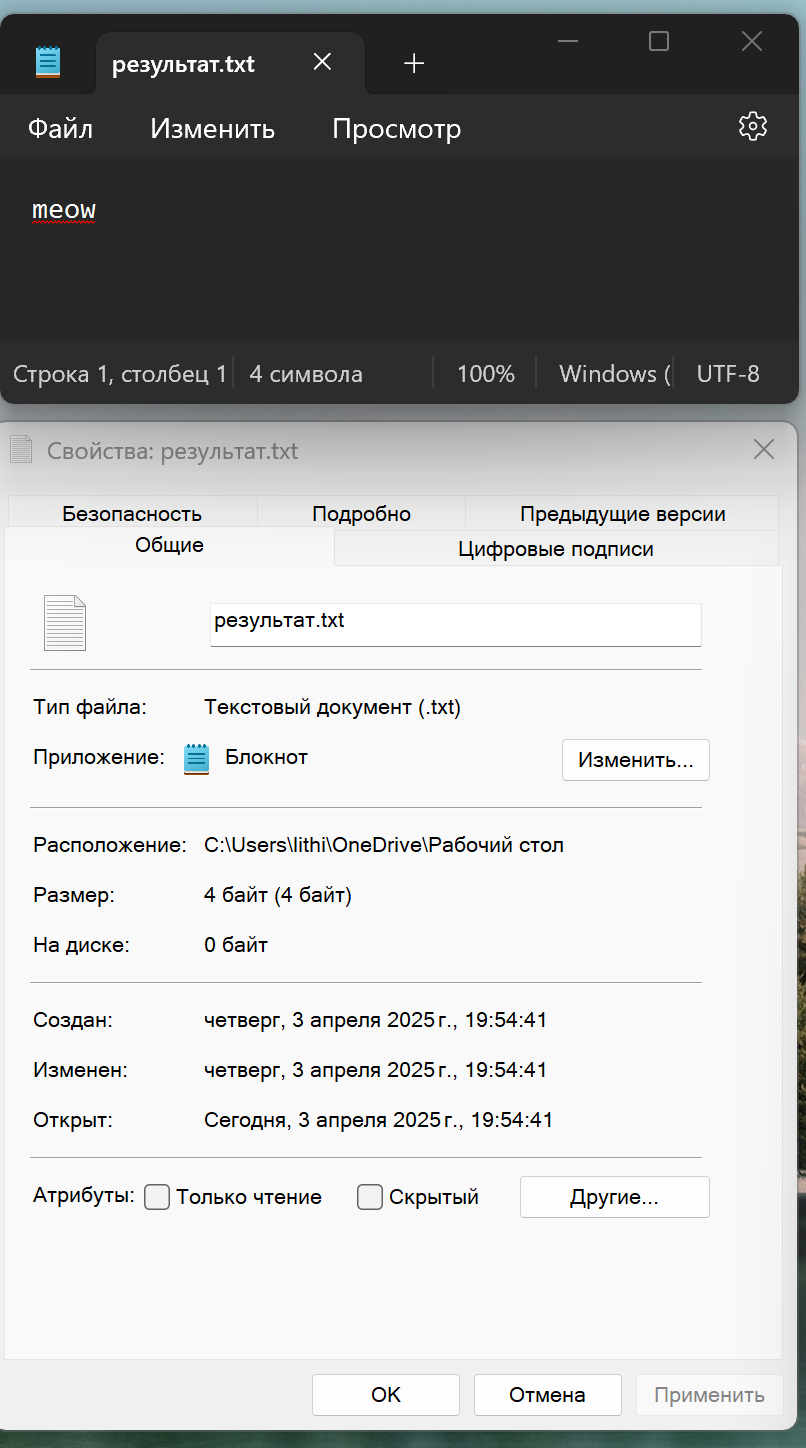
Открытие зашифрованного файла:



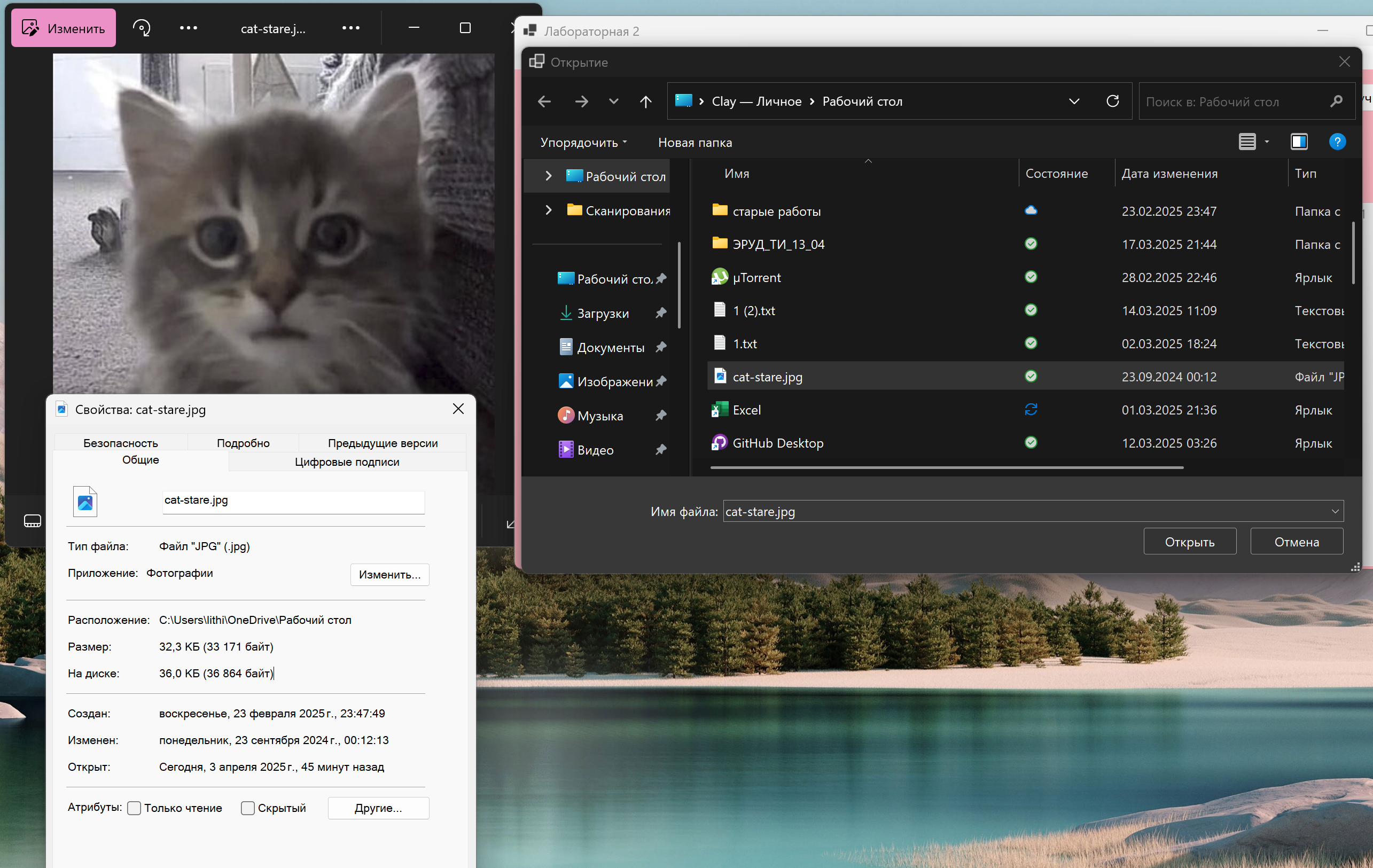
Дешифрование:



Получившийся файл:



Картинка, открытие файла:



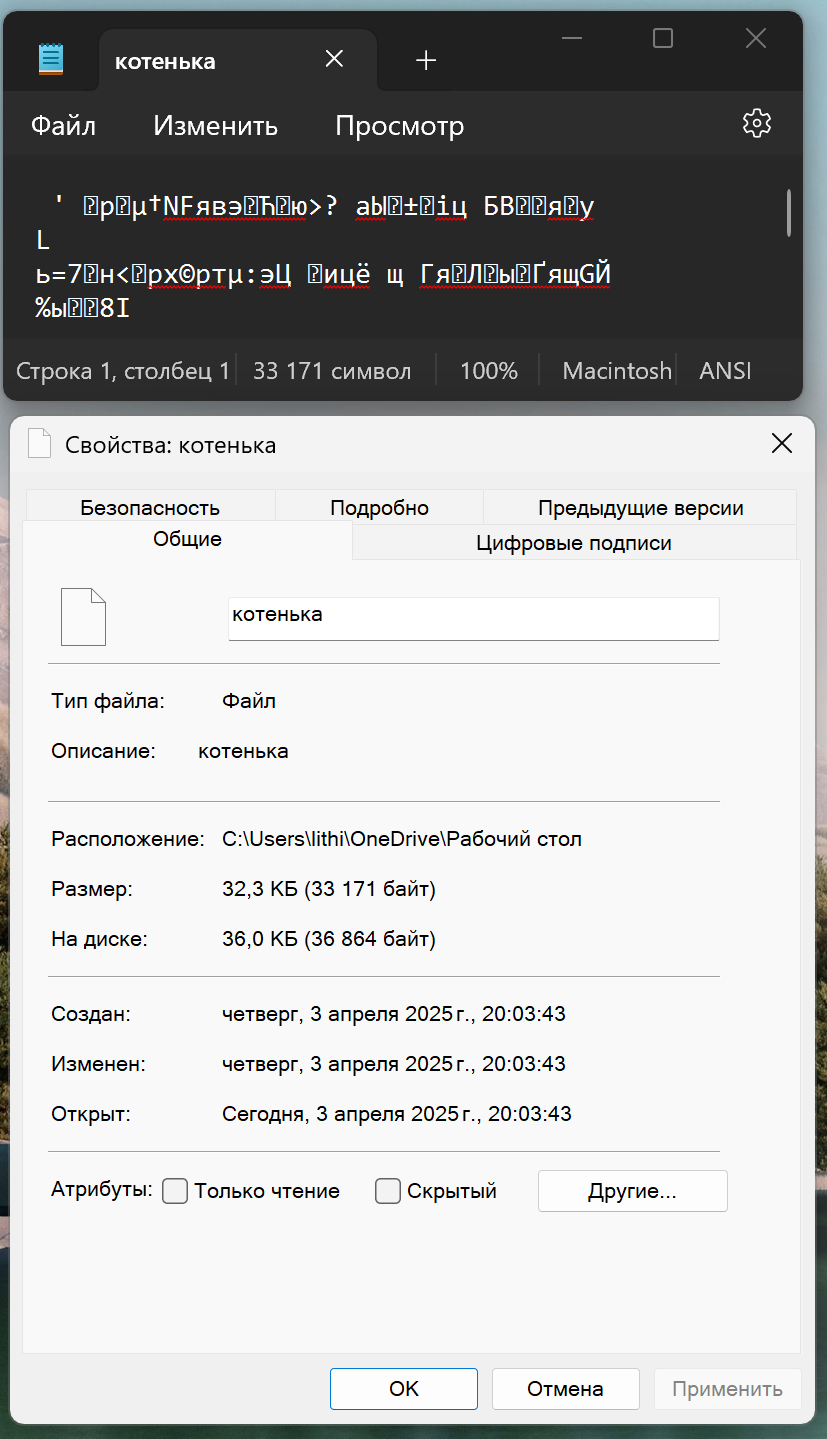
Шифрование:



Сохранение в файл:



Получившийся файл:



Дешифрование:



Получившийся файл:

