УО «Белорусский государственный университет информатики и радиоэлектроники»

Отчет по лабораторной работе №2

по предмету «Теория информации»

Вариант 18

Выполнил:

Наривончик А.М.

Гр. 351004

Проверил:

Болтак С.В.

Минск 2025

**Размер регистра**: 40 бит

**Примитивный многочлен:** *x*40 + *x*21 + *x*19 + *x*2 + 1

На скриншотах тестовый файл открыт в:

1. окне свойств файла
2. окне редактора HxD (*для бинарного отображения файла*)
3. окне необходимого для отображения ПО(*блокнот для текстовых и т.д*.)

Для каждого теста в папке «Тесты» лежит соответствующая Exel таблица состояний регистра.

**Тест 1 (***текст***)**

**Исходный файл**: test 1.txt

**Ключ**: 11111111\_11111111\_11111111\_11111111\_11111111

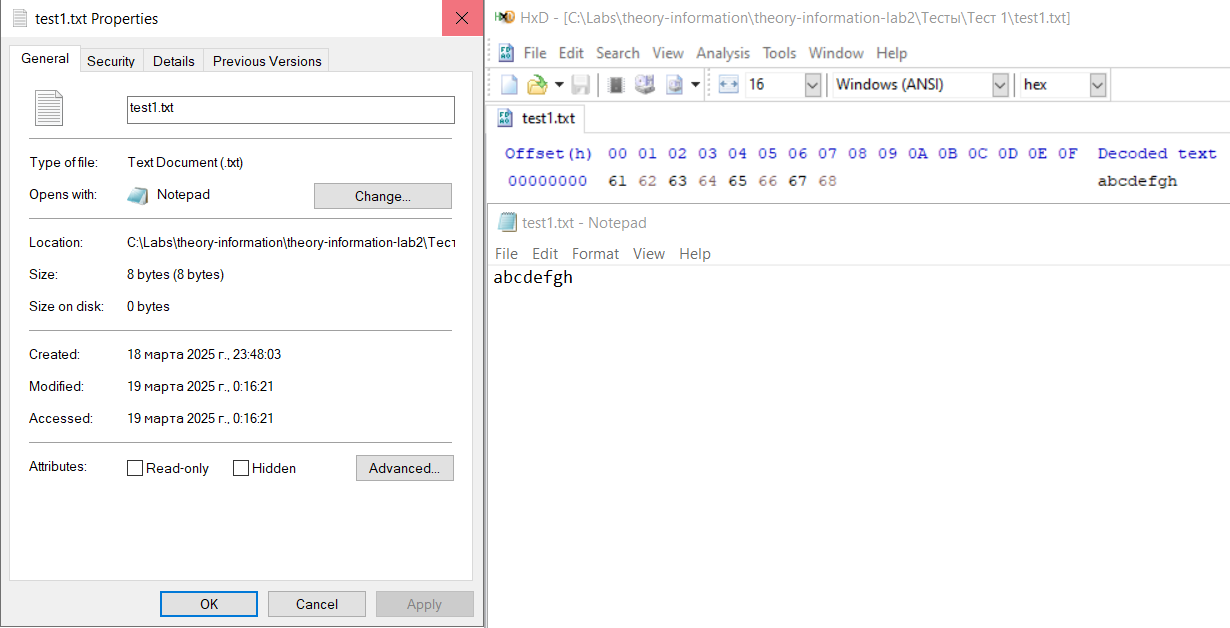


Рисунок 1.1 – исходный файл test1.txt

**Сгенерированный ключ:** 11111111\_11111111\_11111111\_11111111\_11111111\_00110011\_00110011\_00101010

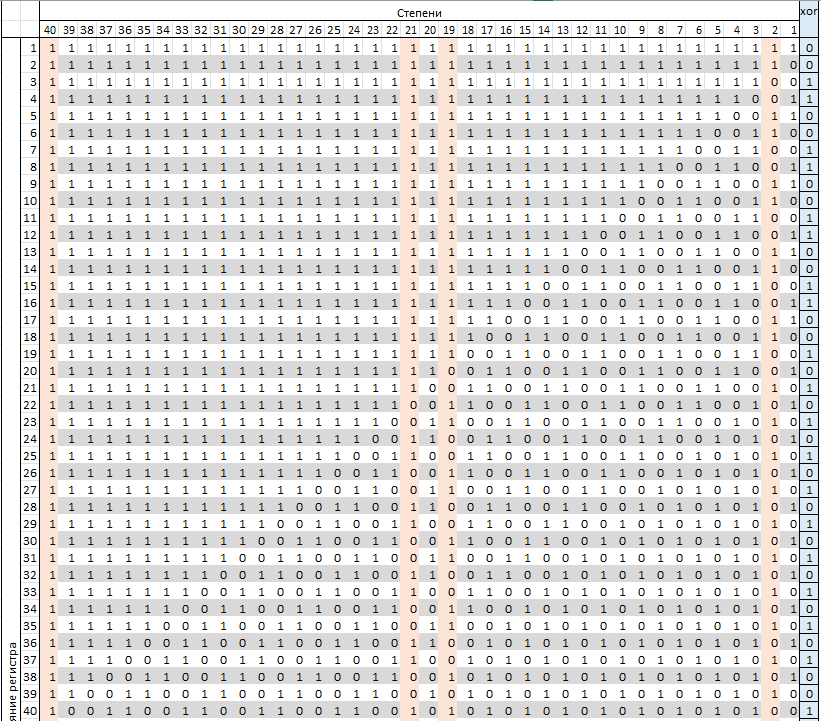


Рисунок 1.2 – таблица состояний регистра (*вдвинутые в регистр биты в синей колонке – это часть сгенерированного ключа начиная с 41-го бита*)

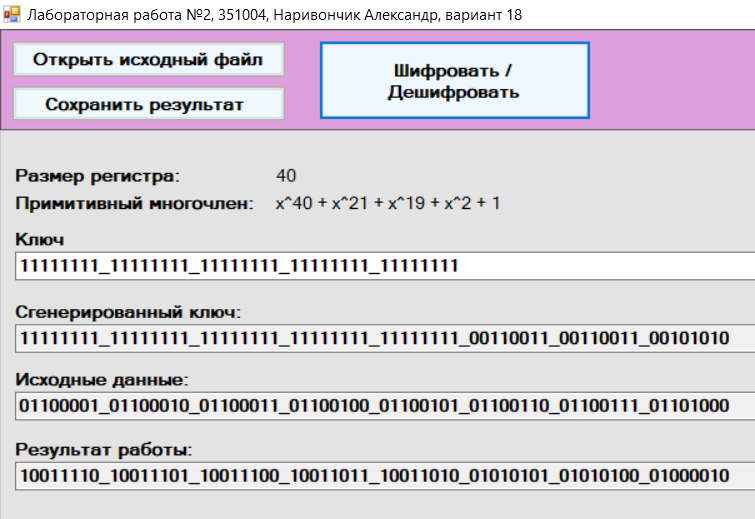


Рисунок 1.3 – шифрование test1.txt

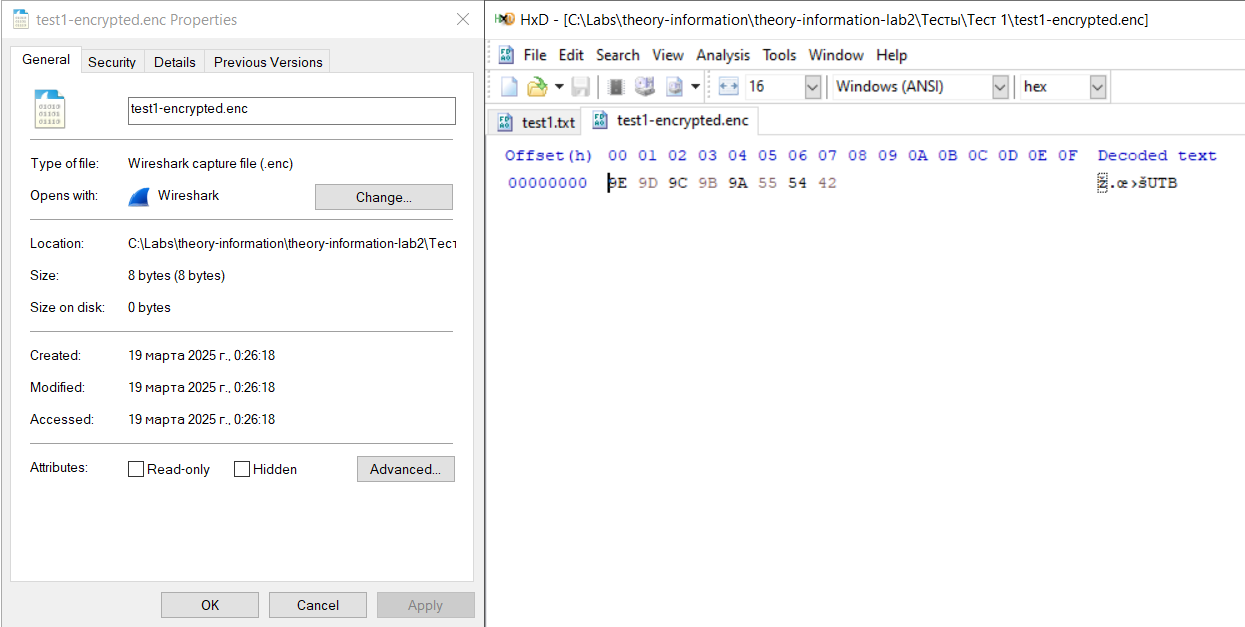


Рисунок 1.4 – зашифрованный файл test1-encrypted

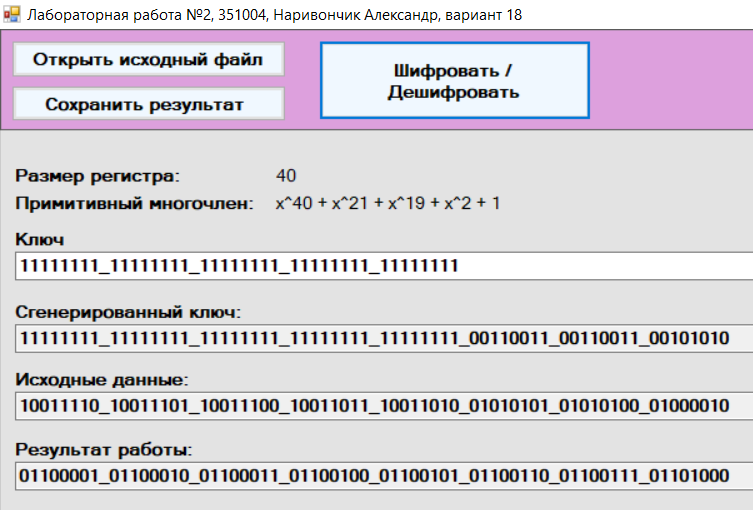


Рисунок 1.5 – дешифрование test1-encrypted

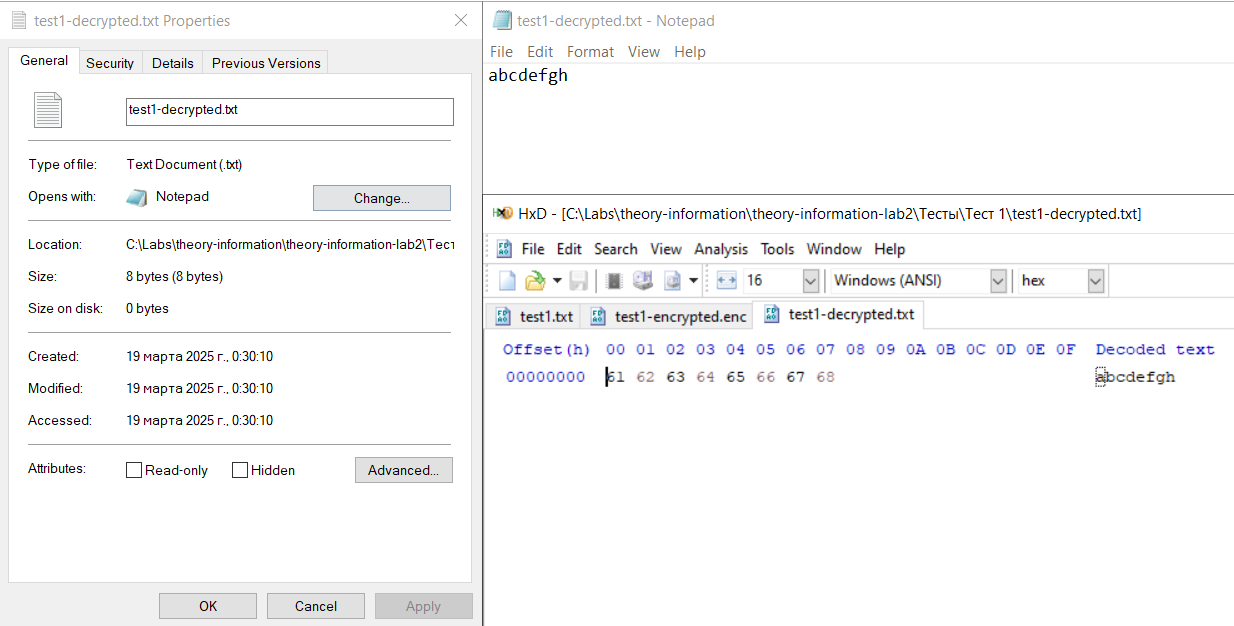


Рисунок 1.6 - дешифрованный файл test1-decrypted.txt

**Тест 2 (***изображение***)**

**Исходный файл**: test 2.jpg

**Ключ**: 10101010\_00000000\_11111111\_11001100\_11100011

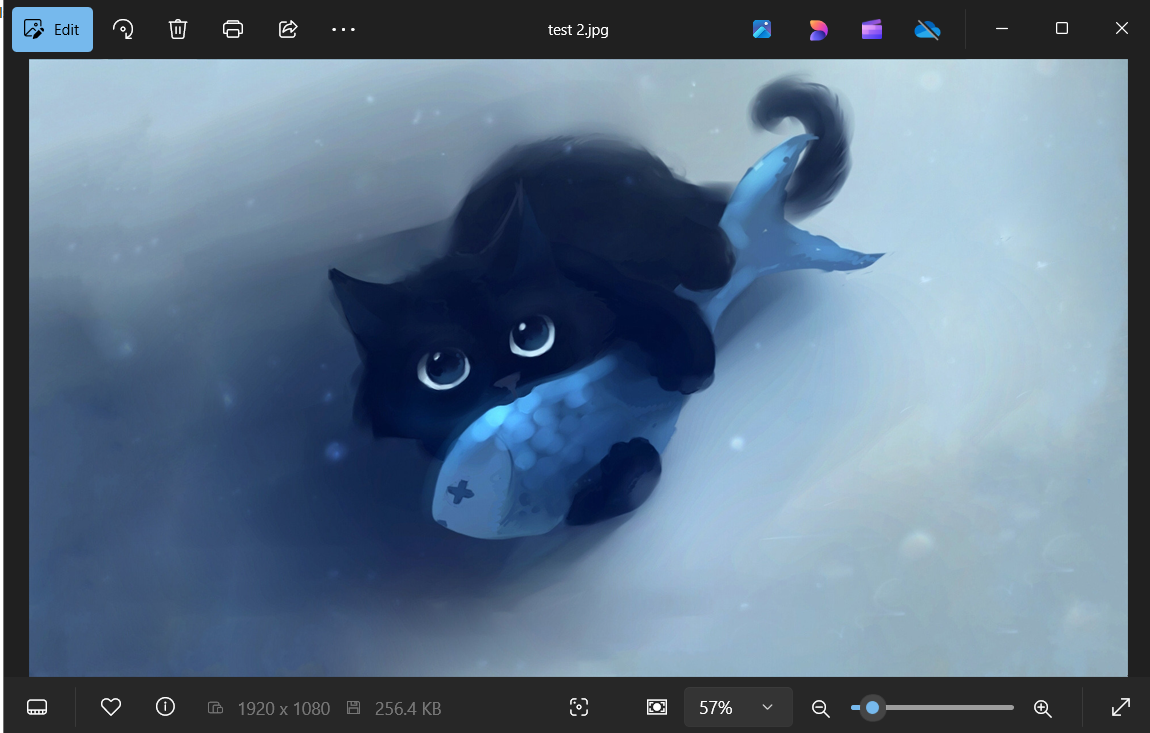


Рисунок 2.1 – исходный файл test 2.jpg

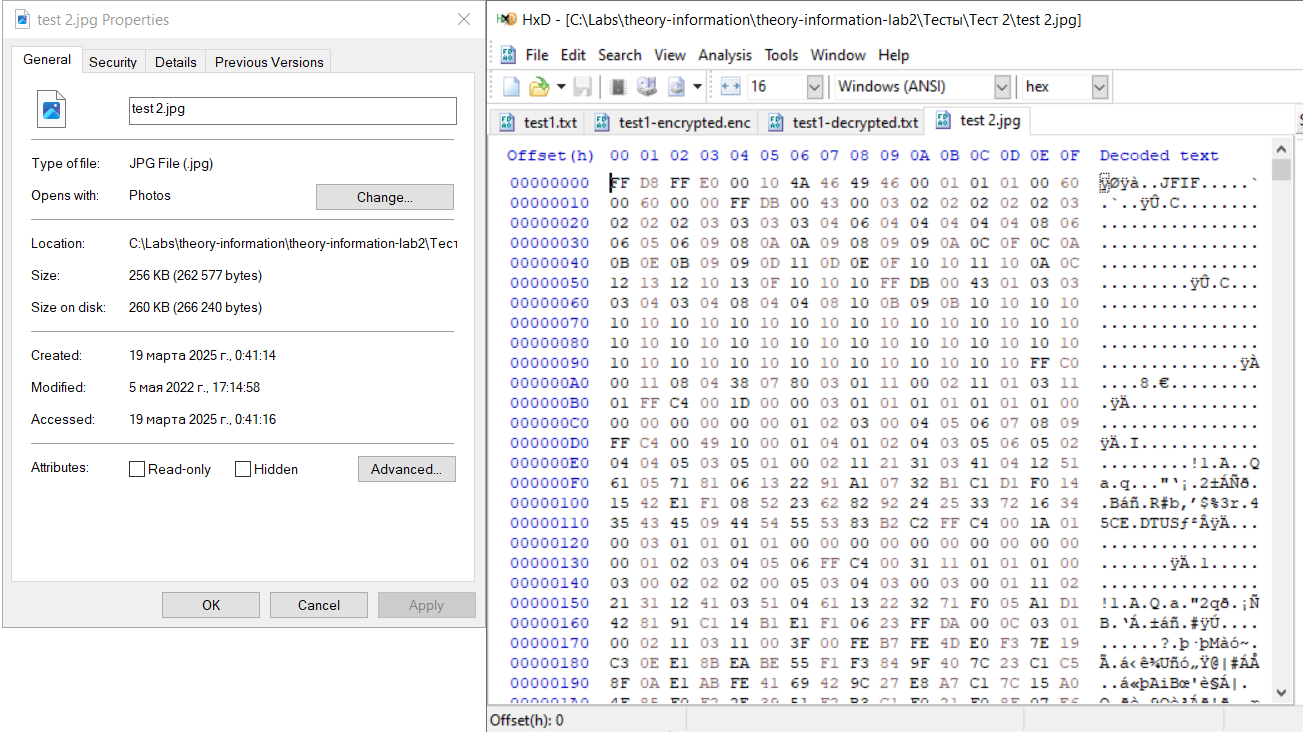


Рисунок 2.2 – исходный файл test2.jpg (*свойства файла и бинарный вид*)

**Сгенерированный ключ (*первые 80 бит и последние 80 бит*):**

10101010\_00000000\_11111111\_11001100\_11100011\_01110001\_10011100\_10100010\_11000011\_01000010\_...\_00010110\_11111001\_00111101\_01010101\_01010000\_01000111\_00110100\_10010011\_01011101\_00101101

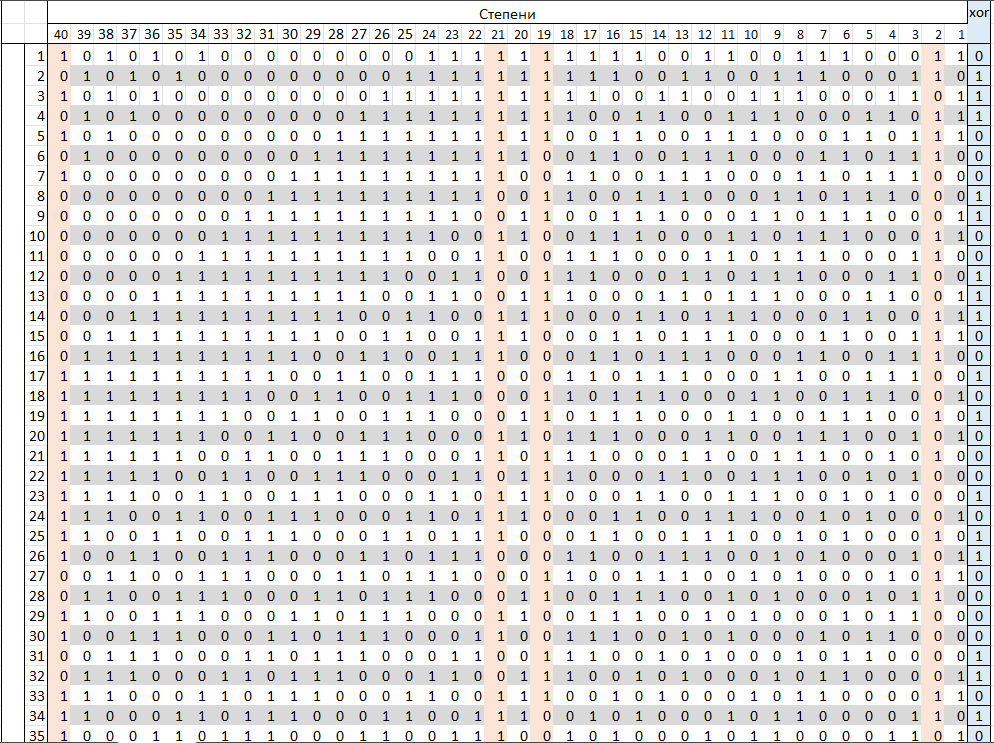


Рисунок 2.3 – таблица состояний регистра (*вдвинутые биты в синей колонке – это часть сгенерированного ключа начиная с 41-го бита*)

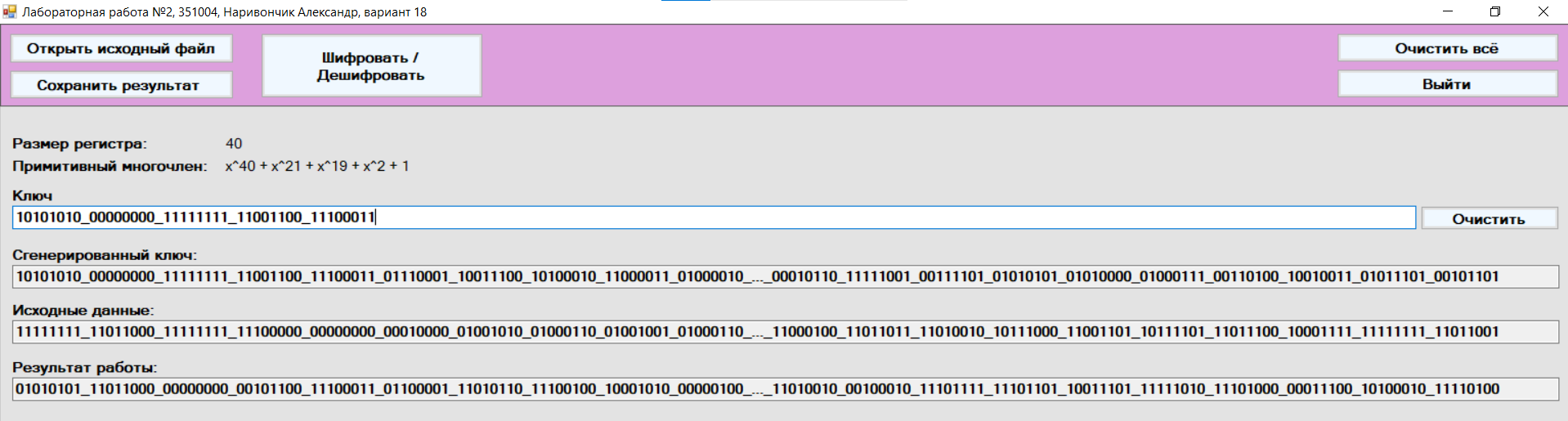


Рисунок 2.4 – шифрование test2.jpg

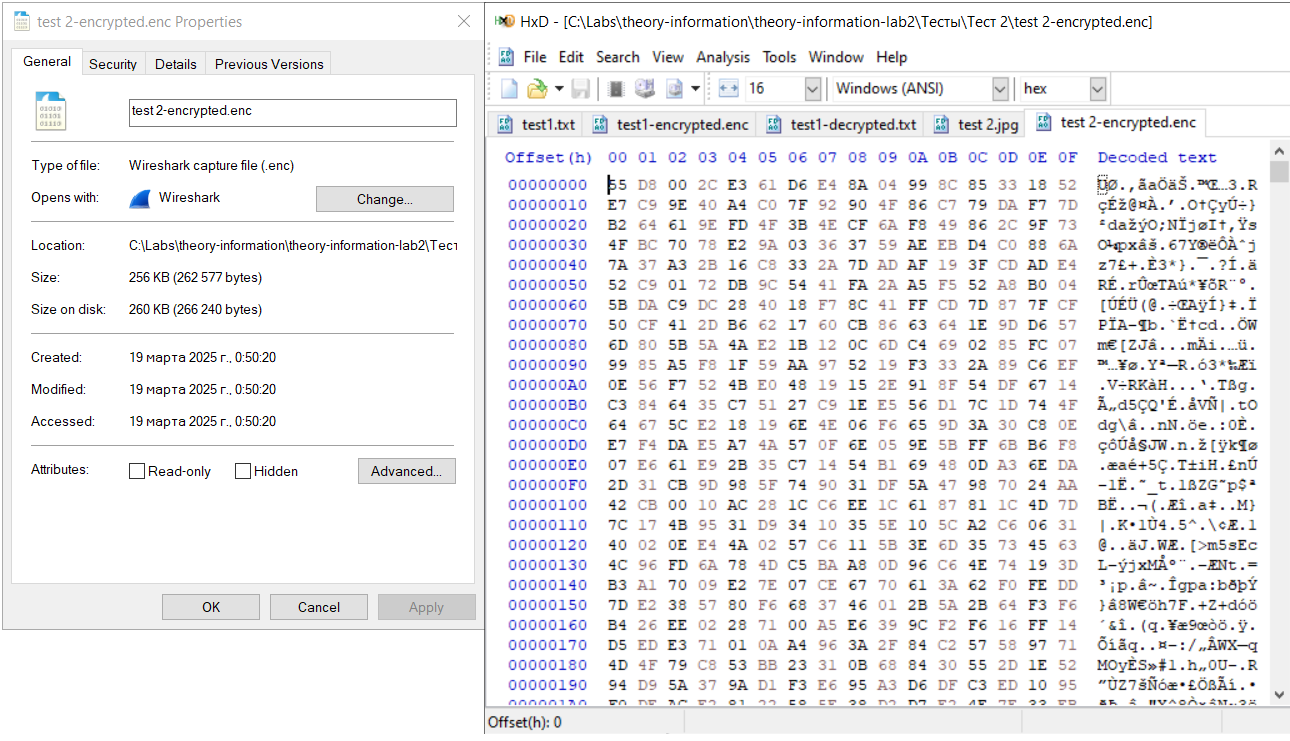


Рисунок 2.5 – зашифрованный файл test2-encrypted

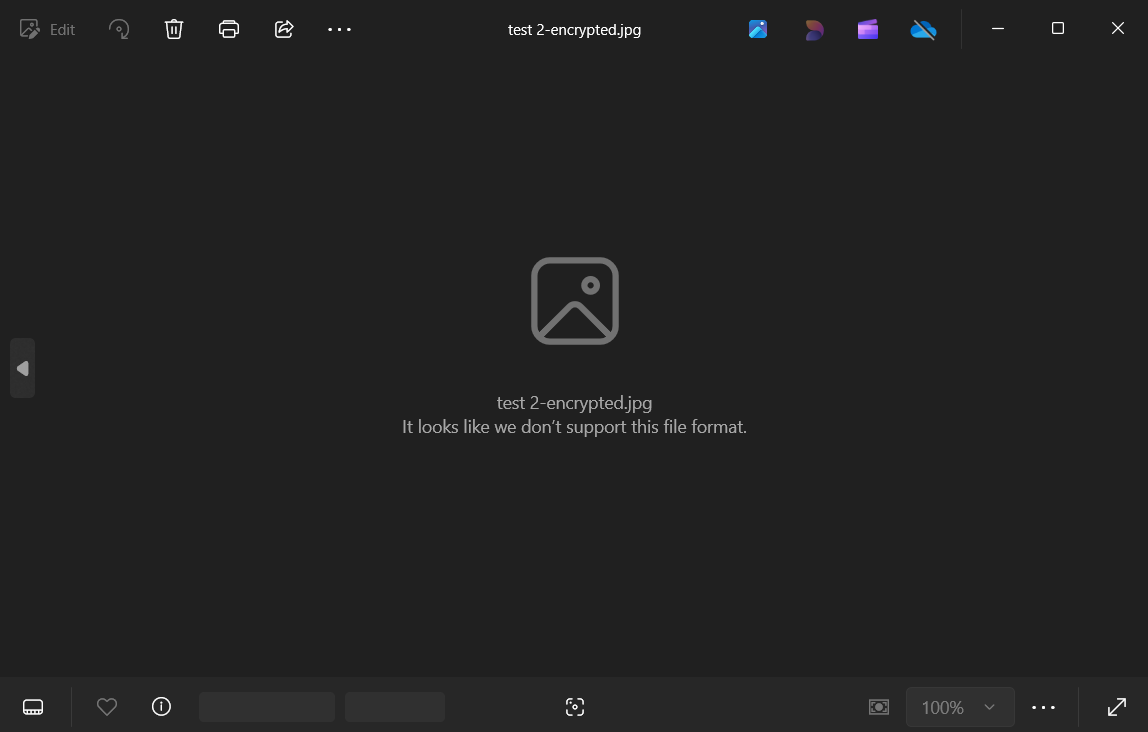


Рисунок 2.6 – зашифрованный test2-encrypted в обозревателе фотографий

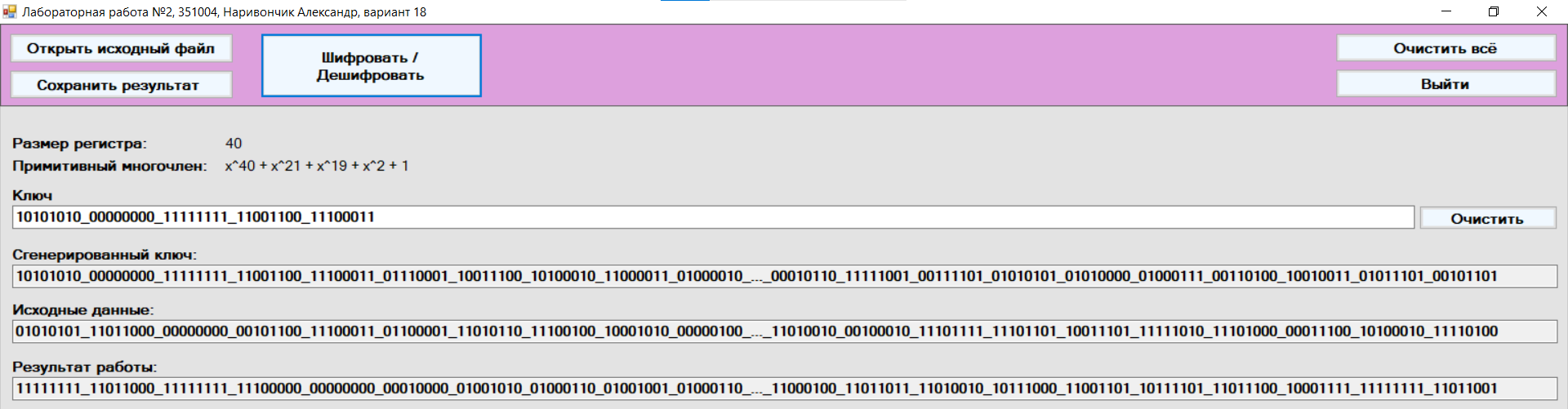


Рисунок 2.7 – дешифрование test2-encrypted

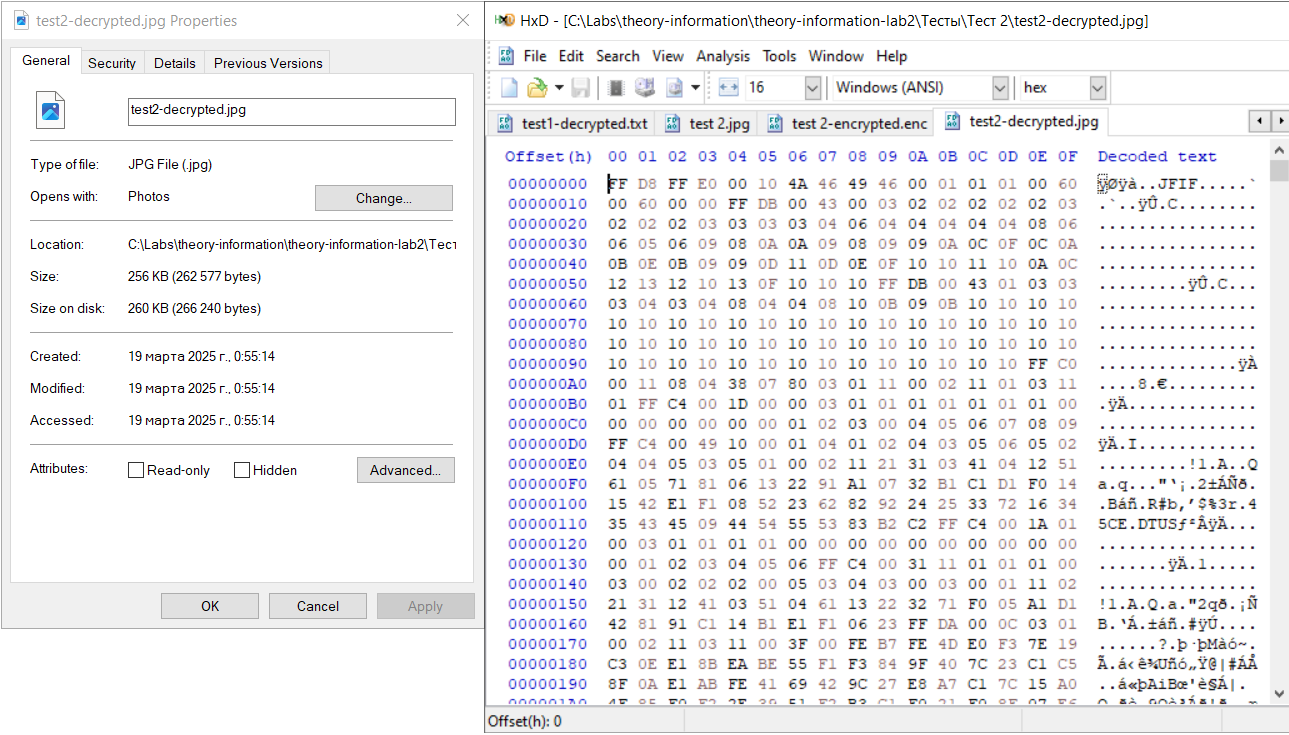


Рисунок 2.8 - дешифрованный файл test2-decrypted.jpg

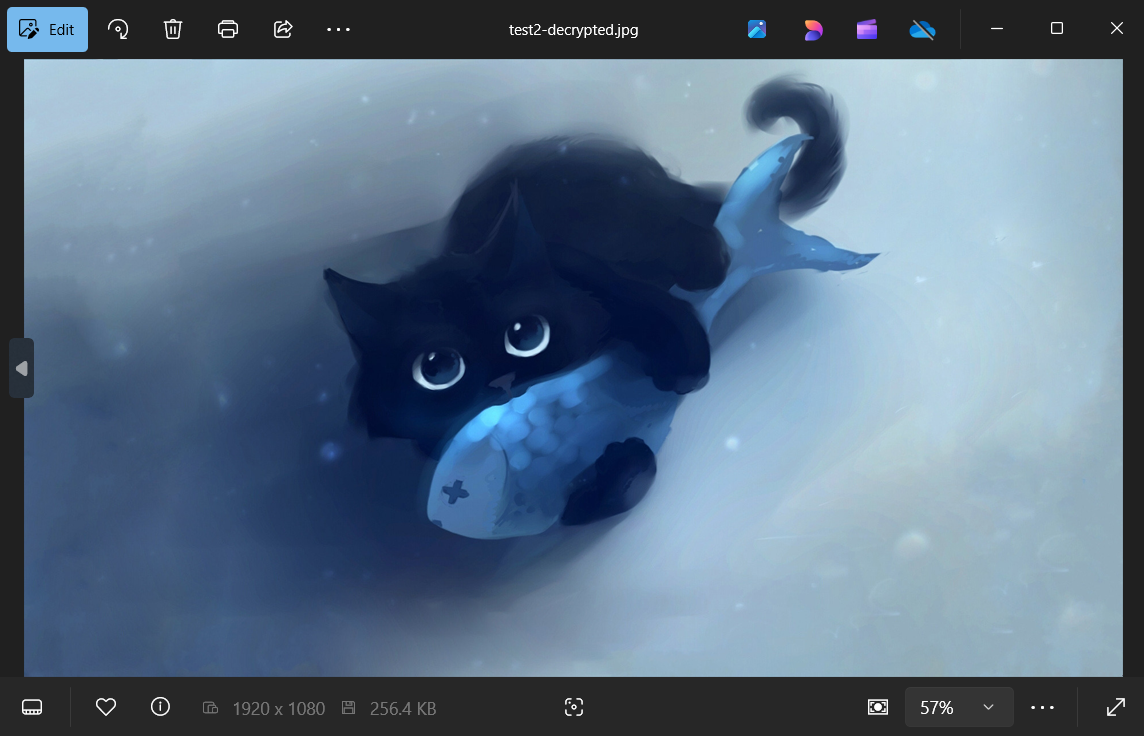


Рисунок 2.9 - дешифрованный файл test2-decrypted.jpg

**Тест 3 (***короткий текст***)**

**Исходный файл**: test 3.txt

**Ключ**: 00110011\_00110011\_00110011\_00110011\_00110011

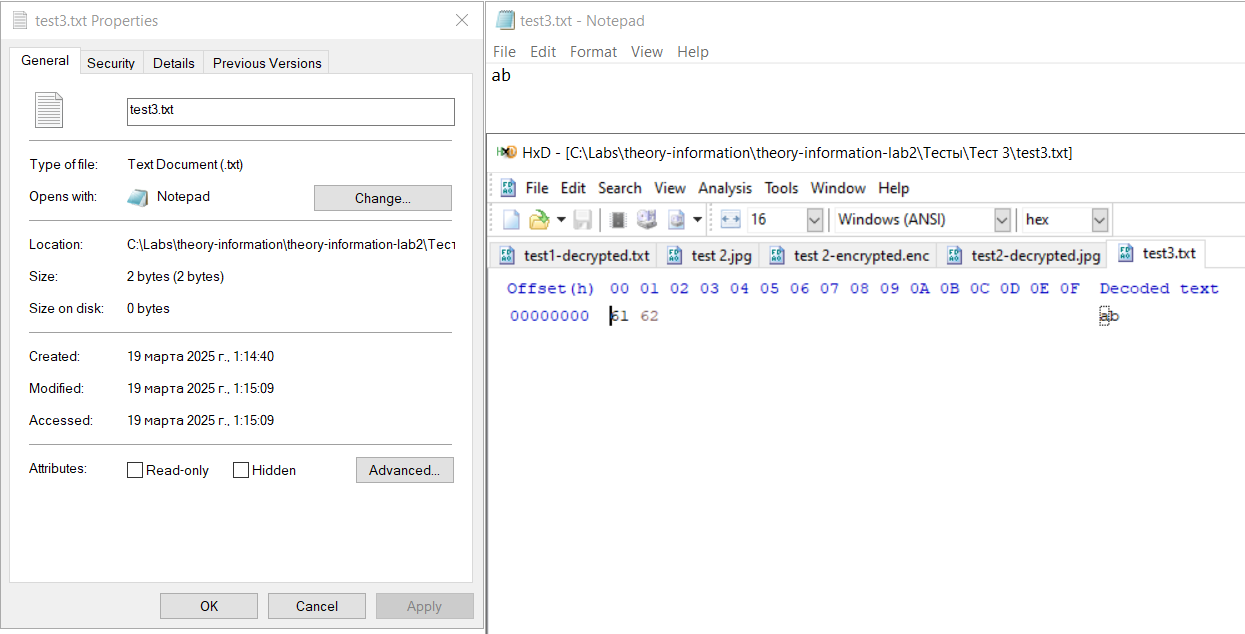


Рисунок 3.1 – исходный файл test3.txt

**Сгенерированный ключ:** 00110011\_00110011

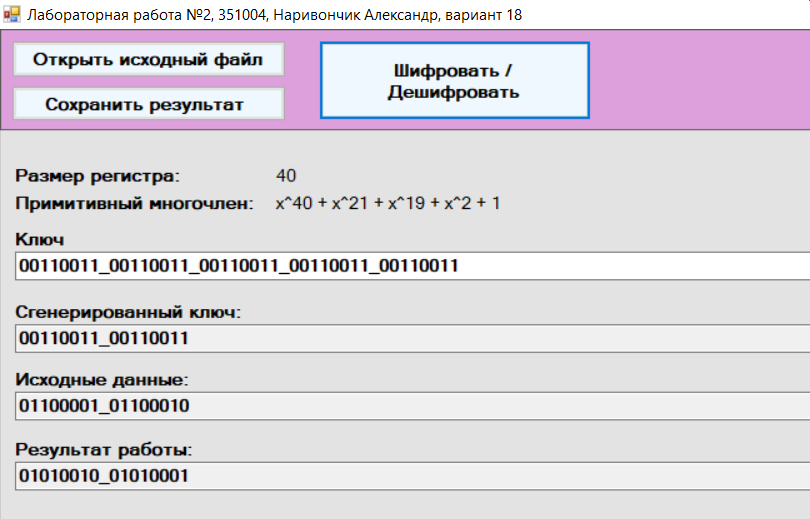


Рисунок 3.2 – шифрование test3.txt

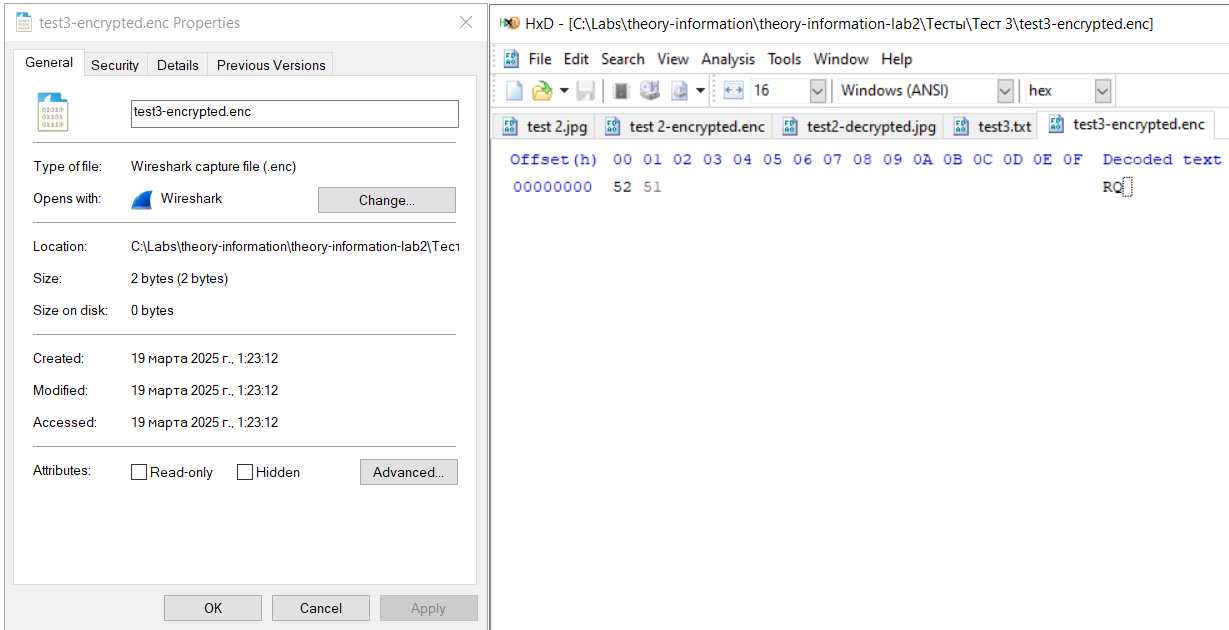


Рисунок 3.3 – зашифрованный файл test3-encrypted

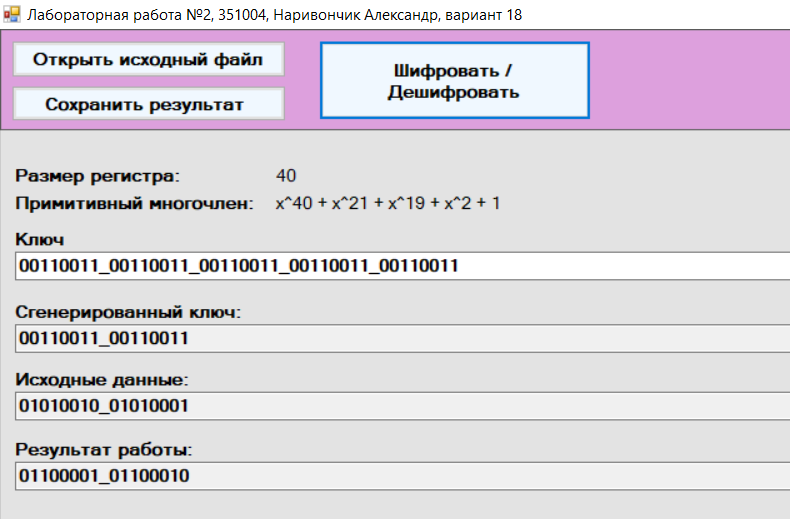


Рисунок 3.4 – дешифрование test3-encrypted

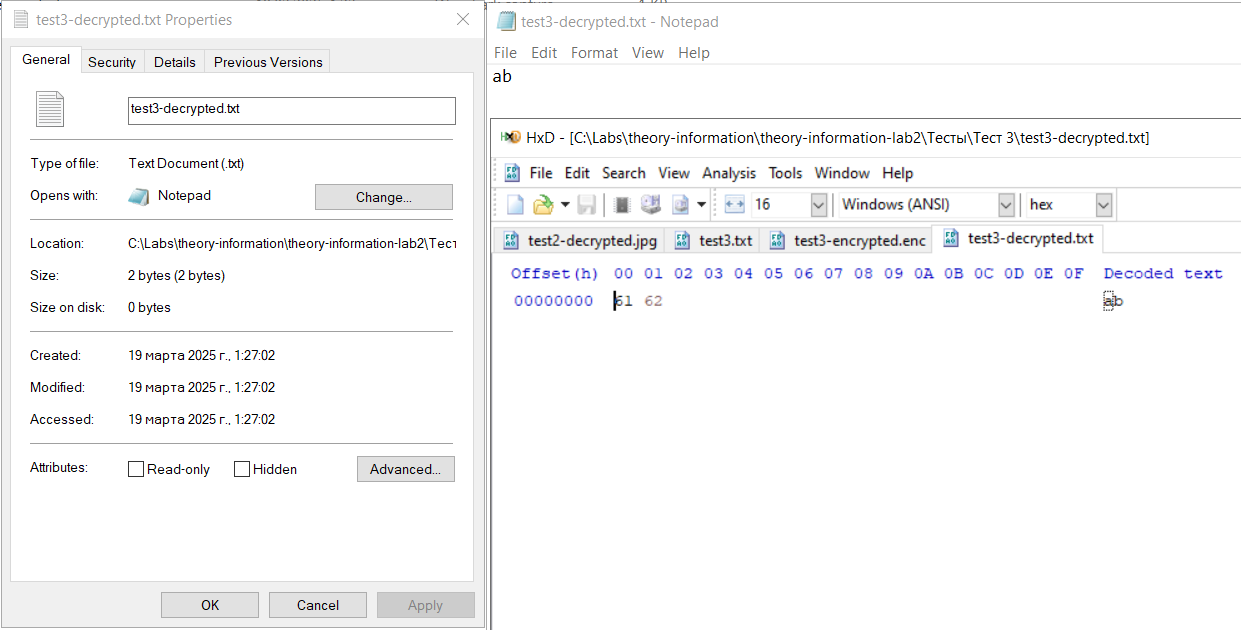


Рисунок 3.5 - дешифрованный файл test3-decrypted.txt

**Тест 4 (***ключ – все нули***)**

**Исходный файл**: test4.txt

**Ключ**: 00000000\_00000000\_00000000\_00000000\_00000000

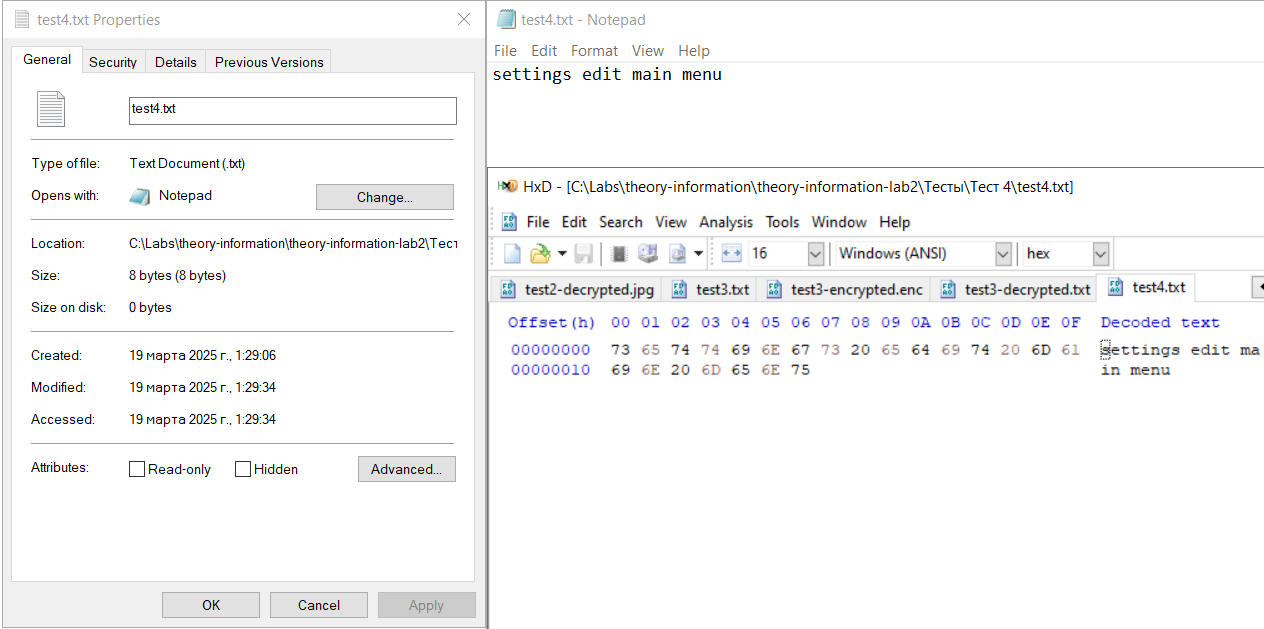


Рисунок 4.1 – исходный файл test4.txt

**Сгенерированный ключ:** 00000000\_00000000\_00000000\_00000000\_00000000\_00000000\_00000000\_00000000\_00000000\_00000000\_...\_00000000\_00000000\_00000000\_00000000\_00000000\_00000000\_00000000\_00000000\_00000000\_00000000

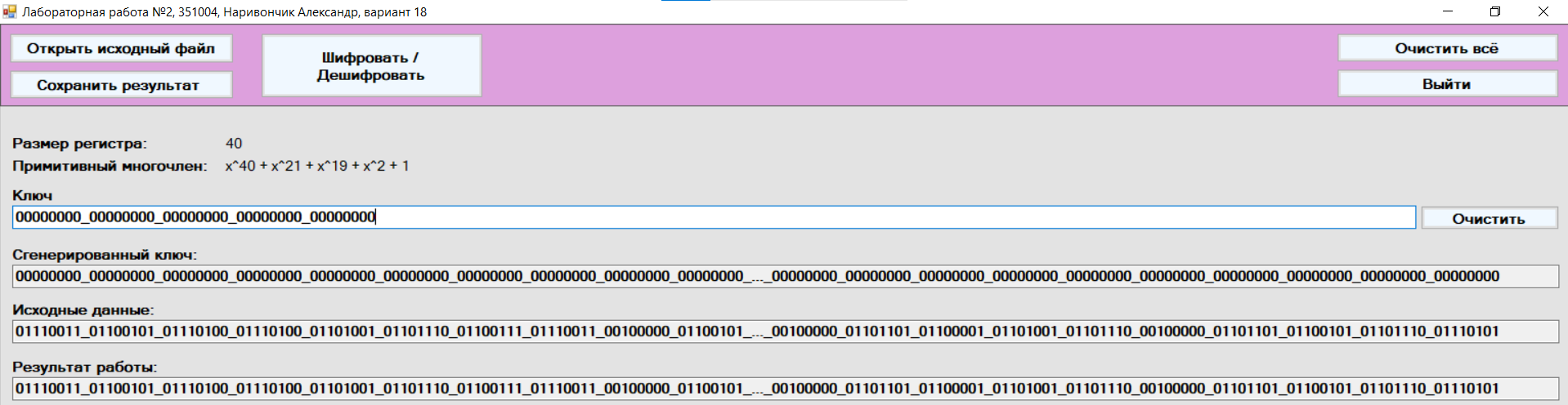


Рисунок 4.2 – шифрование test4.txt

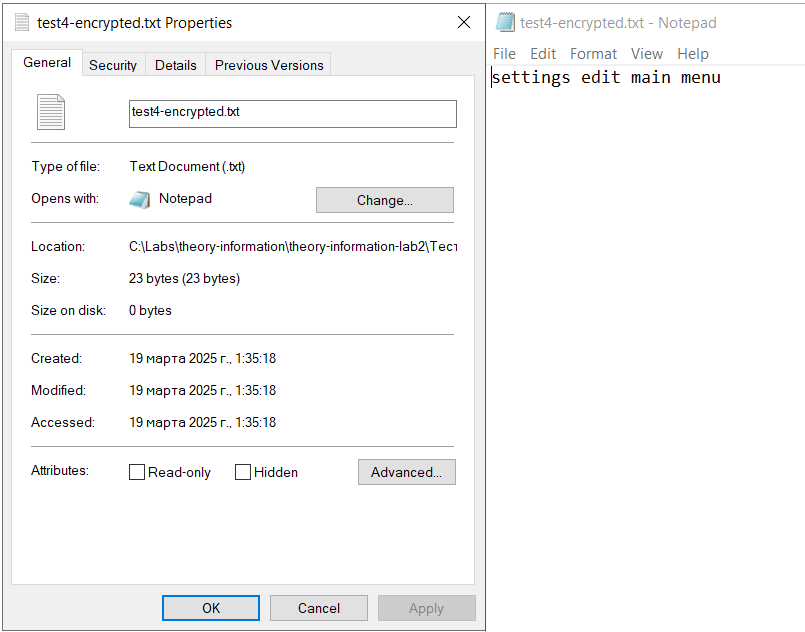
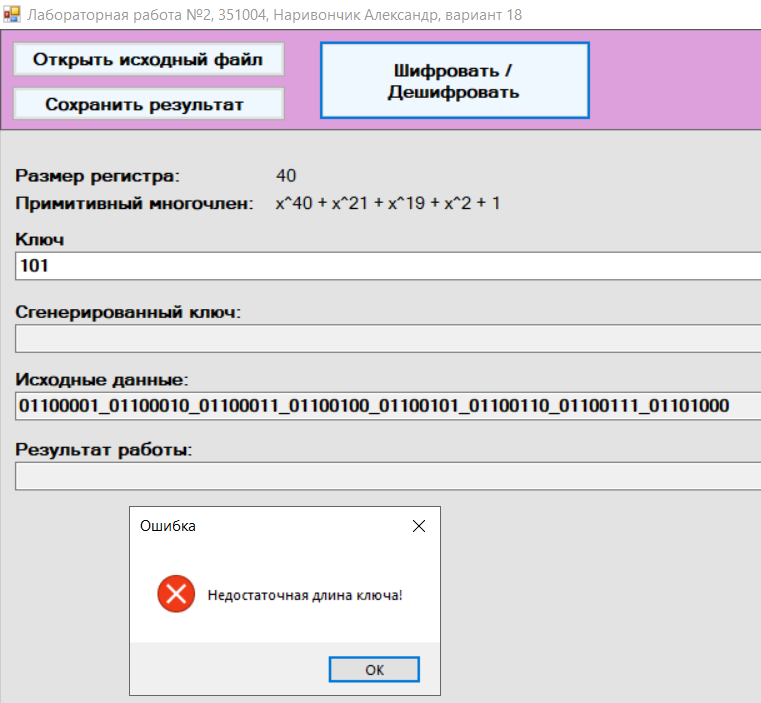


Рисунок 4.3 – зашифрованный файл test4-encrypted

**Тест 5 (***короткий ключ***)**



**Тест 6 (***другие символы в ключе***)**

Компонент TextBox настроен таким образом, что ввод символов, кроме ‘1’ и ‘0’, заблокирован при нажатии на клавиши клавиатуры.