Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

Теория информации

ОТЧЕТ

по лабораторной работе 2

Вариант 13

|  |  |
| --- | --- |
| Выполнил:  Студент гр. 351002 | Филипенко А. С. |
| Проверил: | Болтак С. В. |

Минск 2025

Потоковое шифрование с применением линейного сдвигового регистра с обратной связью

Примитивный многочлен

Тесты

Тест 1

**Состояние регистра:**

11111111111111111111111111111111111

**Ключ:** 111111111111111111111111111111111110011001100110011001100110011001100101101001011010010110100101101001011100010111000101110001011100010111001010001101011100101000110101

**Исходный текст:**

000010111111110110001011100010011000101101000001100010110000000100000100000010111111110100001011101011011000101100000001000010110100110110001011110100010000101110011101

**Зашифрованный текст:**

111101000000001001110100011101100110110100100111111011010110011101100001101011100101100010101110000010000100111011000100110011101000100001000001111001001100000110101000

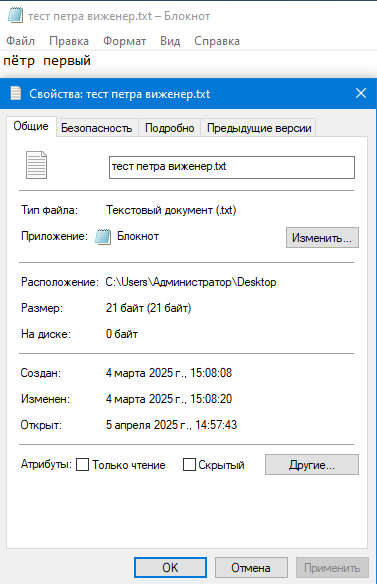


Рис. 1 – Исходные данные

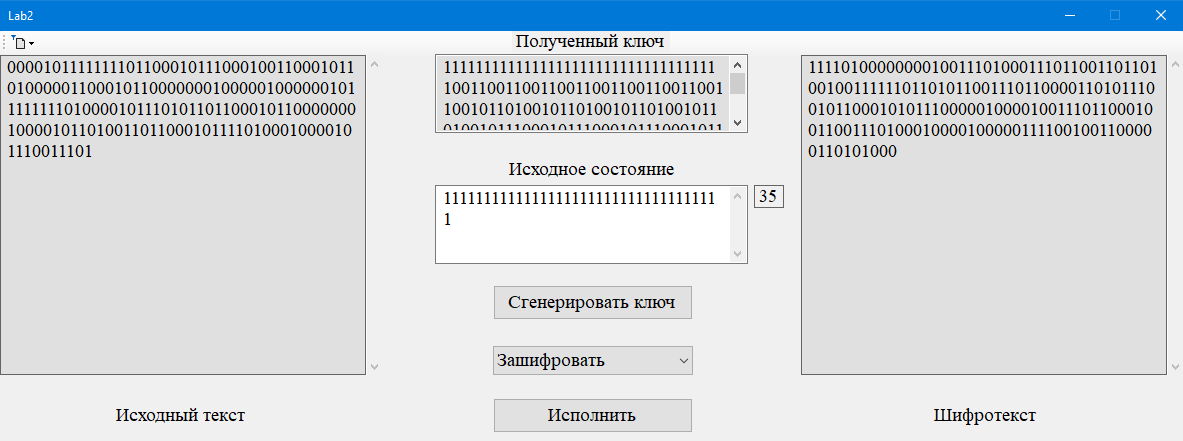


Рис. 2 – Шифрование (после выполнения)

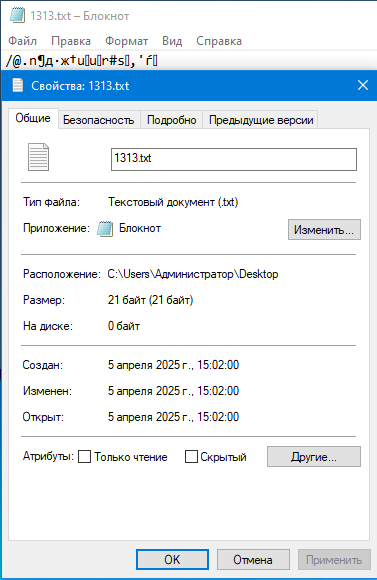


Рис. 3 – Зашифрованные данные

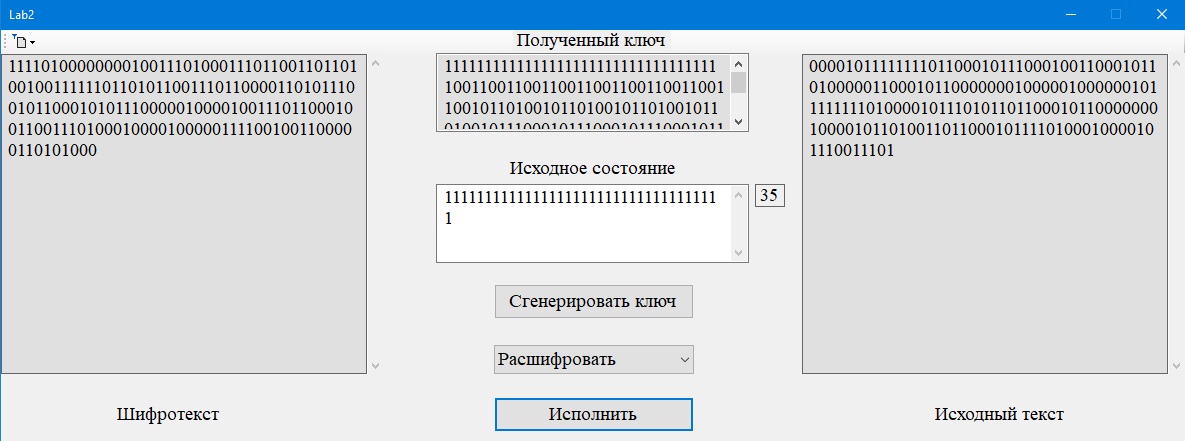


Рис. 4 – Дешифрование (после выполнения)

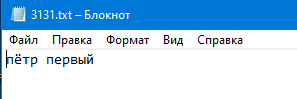


Рис. 5 – Результат дешифрования

Тест 2

**Состояние регистра:**

01010101010110011010011010101010110

**Ключ:** 01010101010110011010011010101010110111011101110000111010010001000100100111001001

...

10100111010110011000111111111011011011110010001111000001100110010010010011010000

**Исходный текст:**

10100100000010100010001001100010101101001000110001110100011011001011000010100100

...

00000100000001000000010000000100000001000000010000000100000001001011000001010000

**Зашифрованный текст:**

11110001010100111000010011001000011010010101000001001110001010001111100101101101

...

10100011010111011000101111111111011010110010011111000101100111011001010010000000

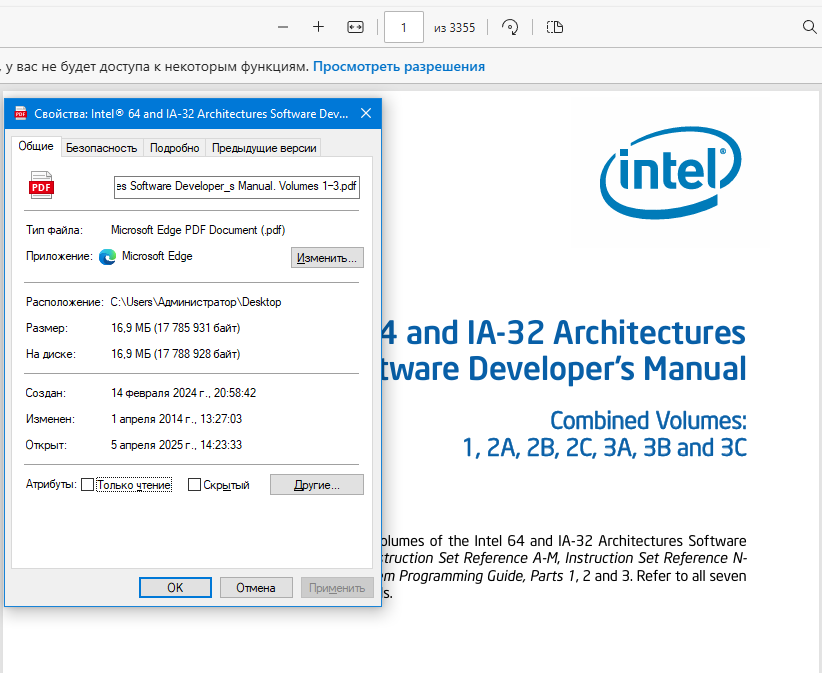


Рис. 6 – Исходные данные

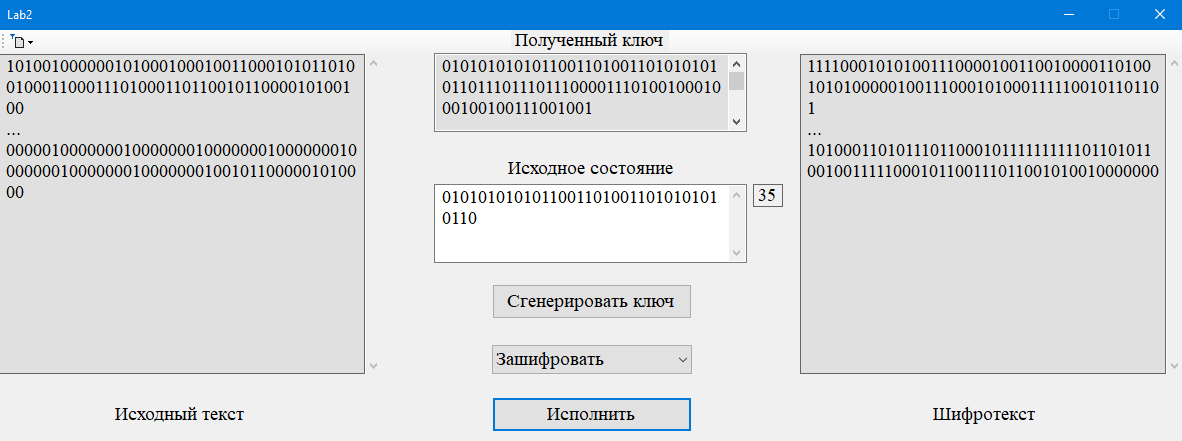


Рис. 7 – Шифрование (после выполнения)

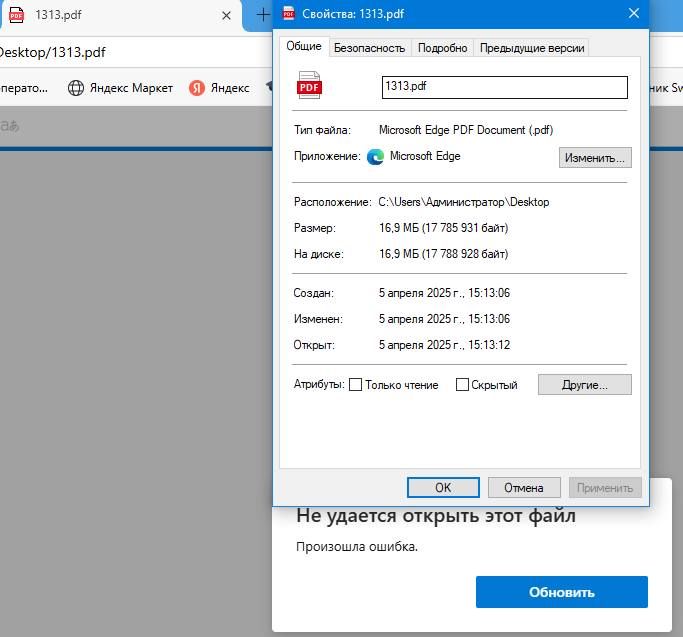


Рис. 8 – Зашифрованные данные

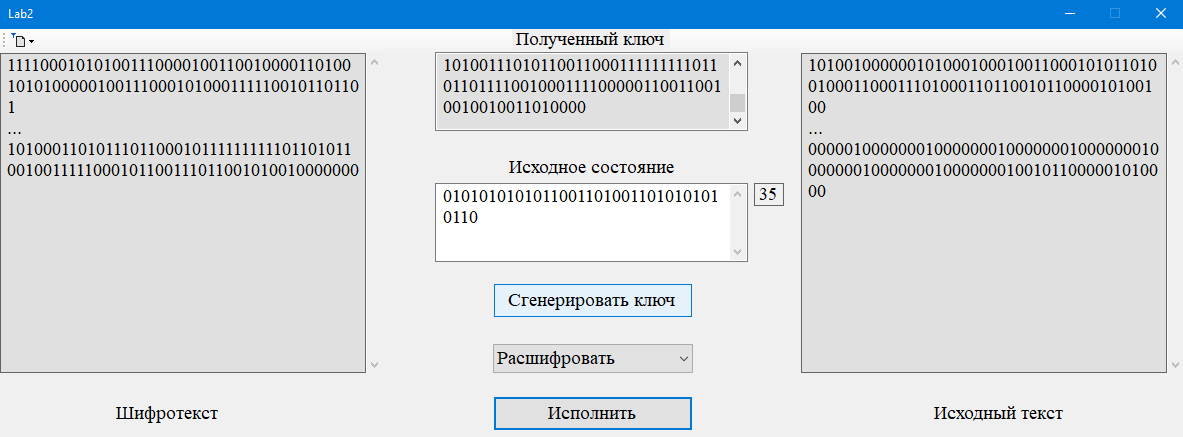


Рис. 9 – Дешифрование (после выполнения)

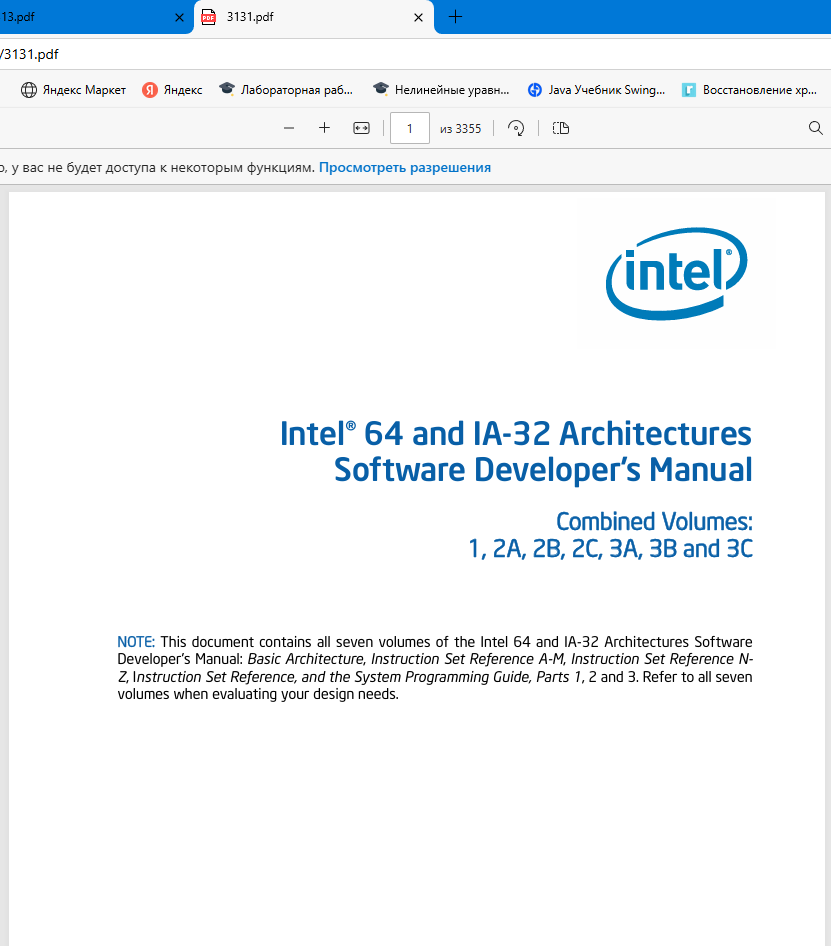


Рис. 10 – Результат дешифрования

Тест 3

**Состояние регистра:**

11111111111111111111000000000000000

**Ключ:** 11111111111111111111000000000000000110011001100110011000000000000000001111000011

...

10000000011100010100010010101100111010101010011111011111010001001011000100010000

**Исходный текст:**

00000000000000000000000000101000011001100010111010011110000011101000111000101110

...

01100110101011001110110001110100001011001000110001110100100011000000110000001100

**Зашифрованный текст:**

11111111111111111111000000101000011111111011011100000110000011101000110111101101

...

11100110110111011010100011011000110001100010101110101011110010001011110100011100

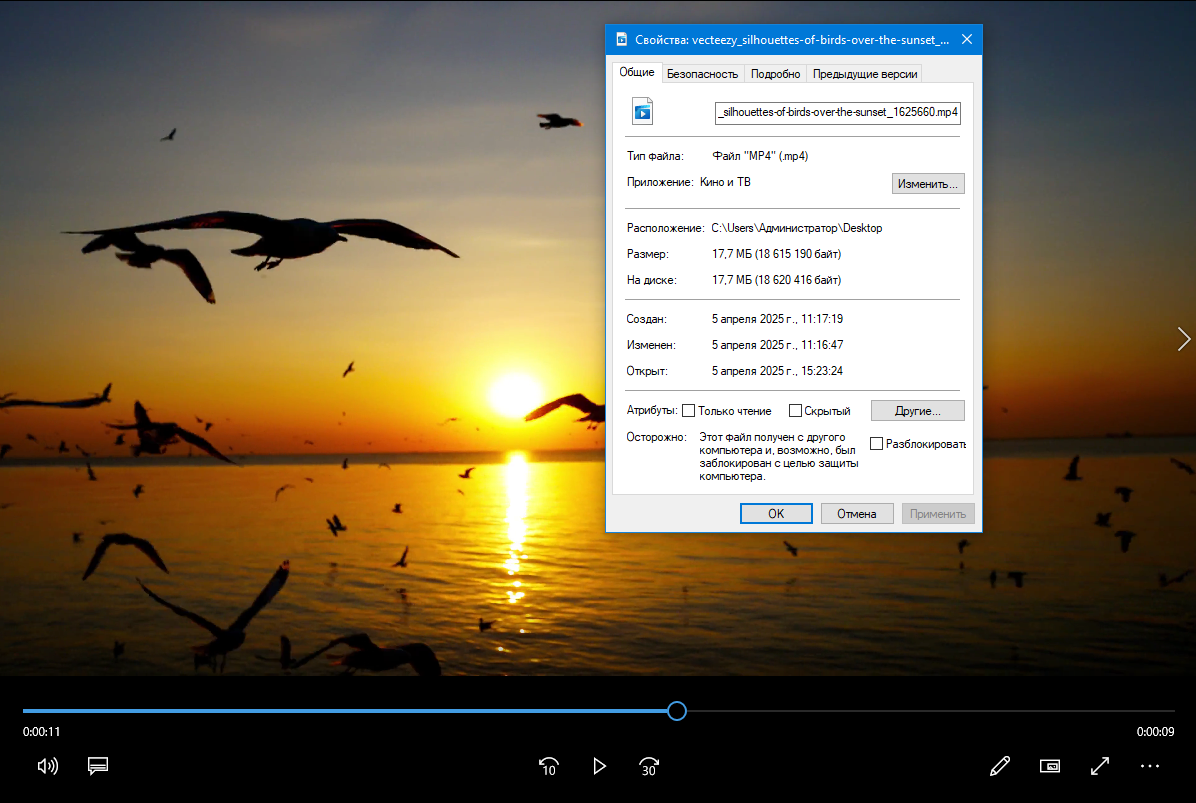


Рис. 11 – Исходные данные

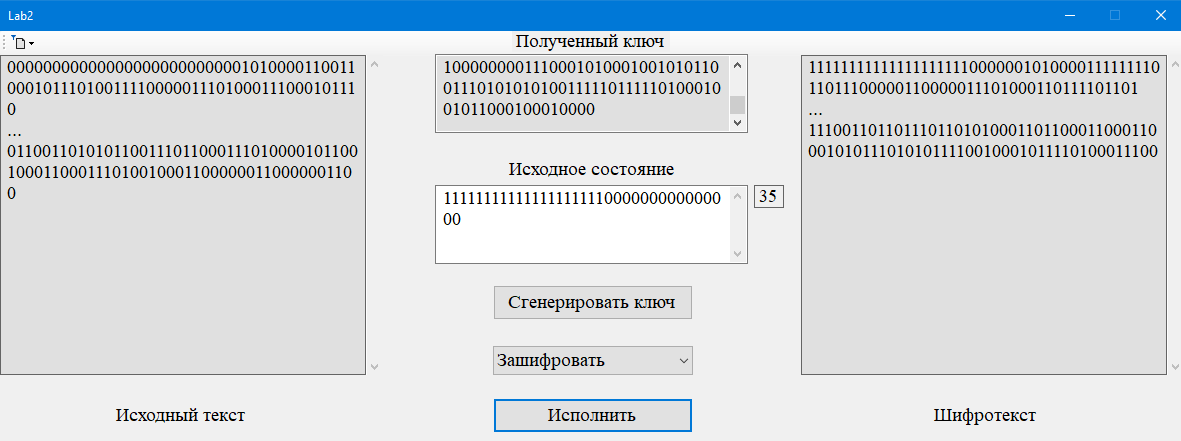


Рис. 12 – Шифрование (после выполнения)

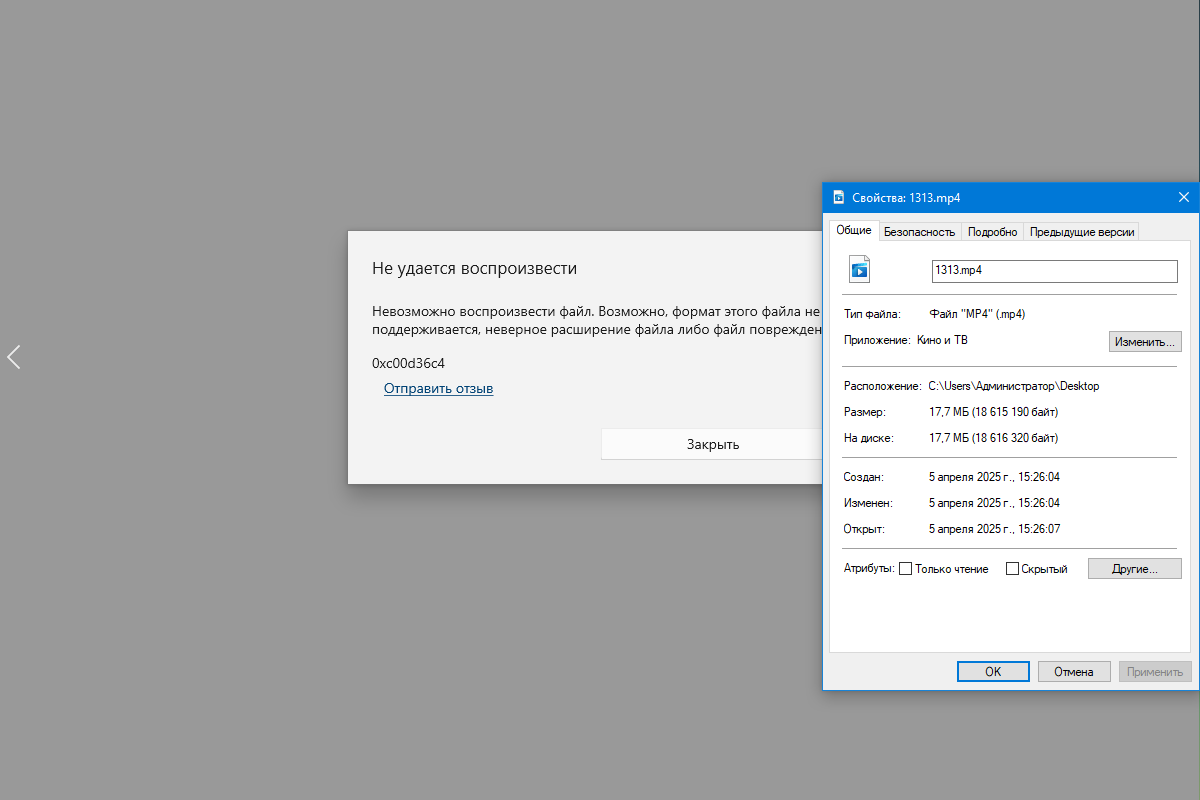


Рис. 13 – Зашифрованные данные

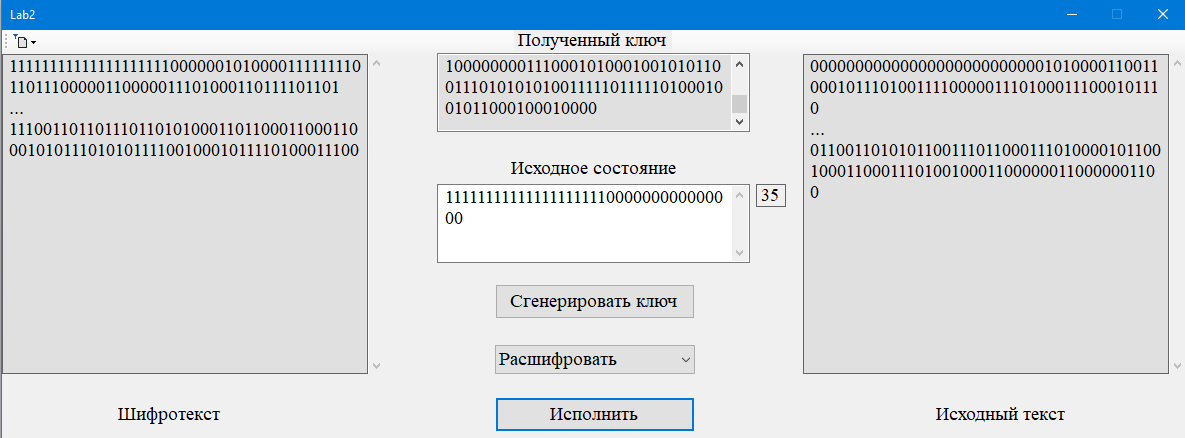


Рис. 14 – Дешифрование (после выполнения)

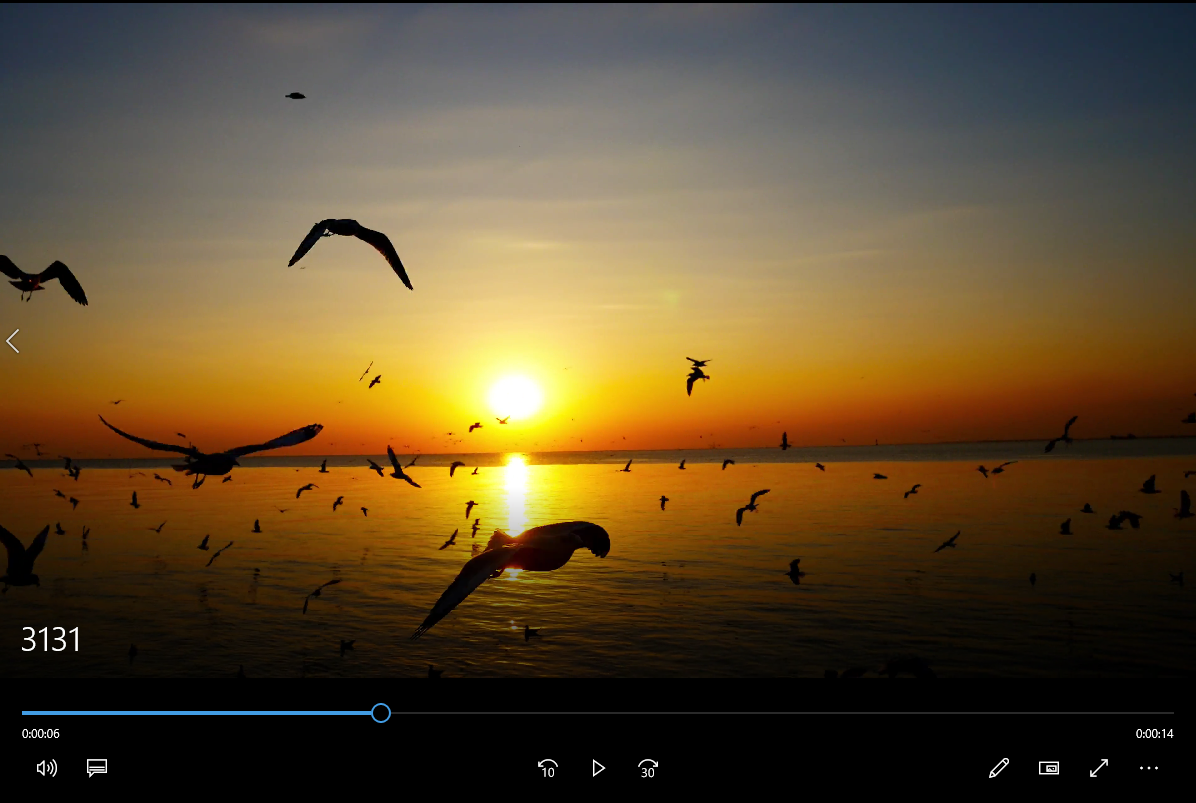


Рис. 15 – Результат дешифрования

Критические ситуации

**Состояние регистра:**

11111111111111111111000000000000000

**Ключ:**

-

**Исходный текст:**

- Ошибка, вызванная большим размером файла

**Зашифрованный текст:**

-

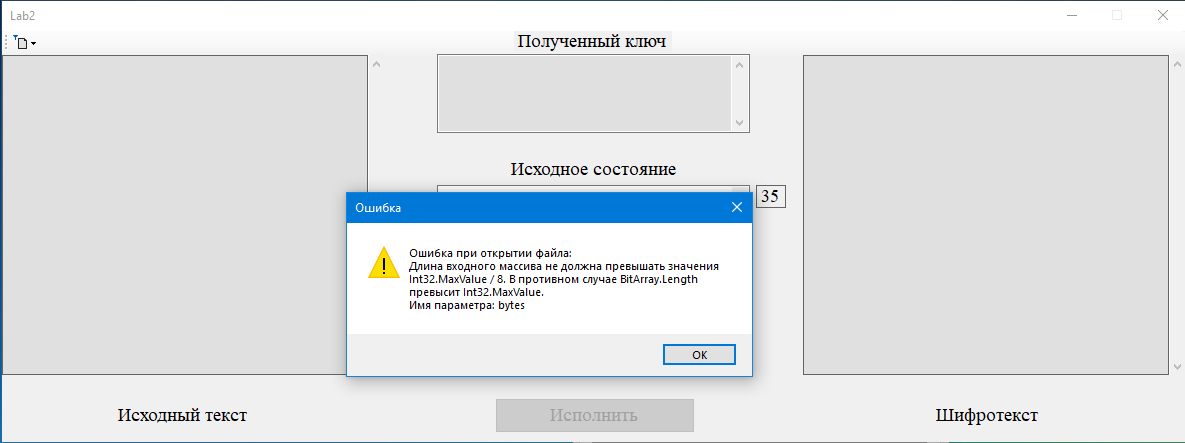


Рис. 16 – Критическая ситуация 1

**Состояние регистра:**

11111111111111111111000000000000000

**Ключ:**

11111111111111111111000000000000000110011001100110011000000000000000001111000011

...

10000000011100010100010010101100111010101010011111011111010001001011000100010000

**Исходный текст:**

00000000000000000000000000101000011001100010111010011110000011101000111000101110

...

01100110101011001110110001110100001011001000110001110100100011000000110000001100

**Зашифрованный текст:**

- Ошибка, вызванная сохранением пустого файла

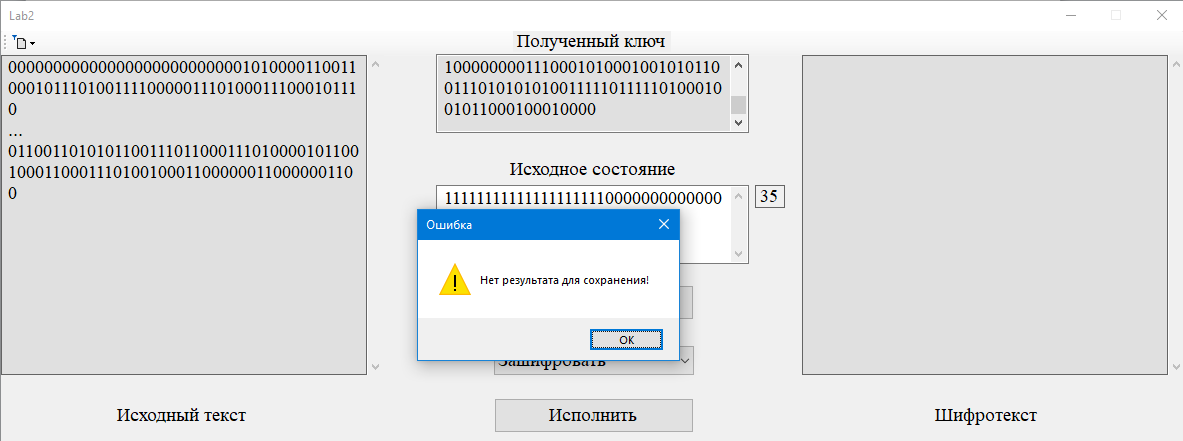


Рис. 17 – Критическая ситуация 2