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:**

110100001011111111010001100100011101000110000010110100011000000000100000110100001011111111010000101101011101000110000000110100001011001011010001100010111101000010111001

**Зашифрованный текст:**

001011110100000000101110011011100011011111100100101101111110011001000101011101010001101001110101000100000001010001000101000101010111011100011011101111100001101010001100

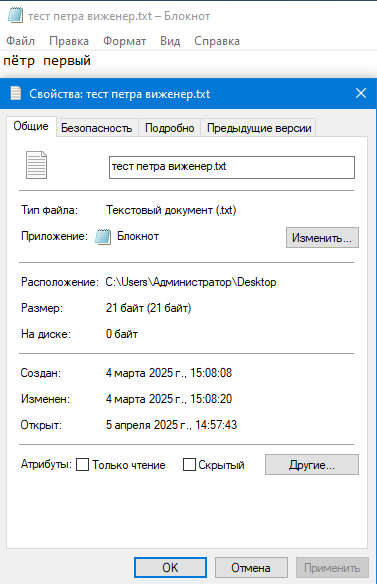


Рис. 1 – Исходные данные

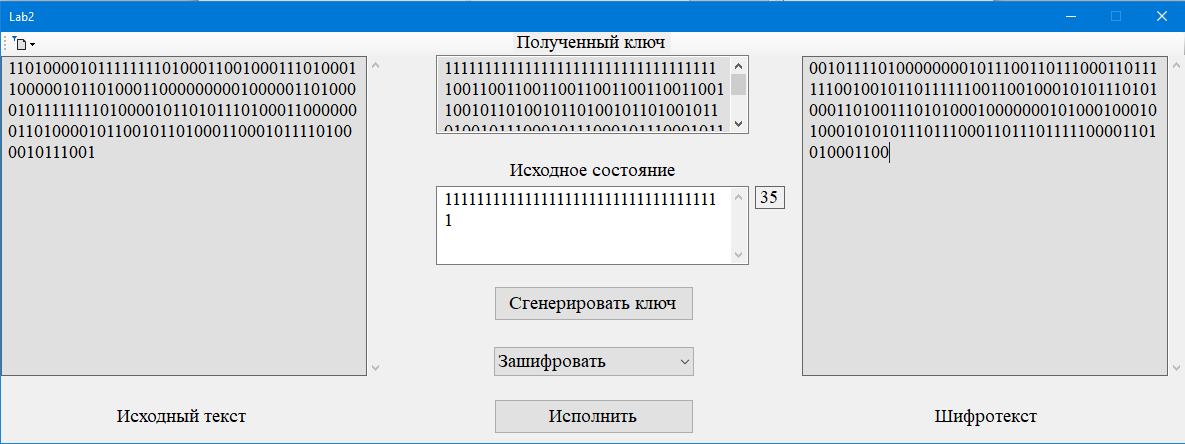


Рис. 2 – Шифрование (после выполнения)

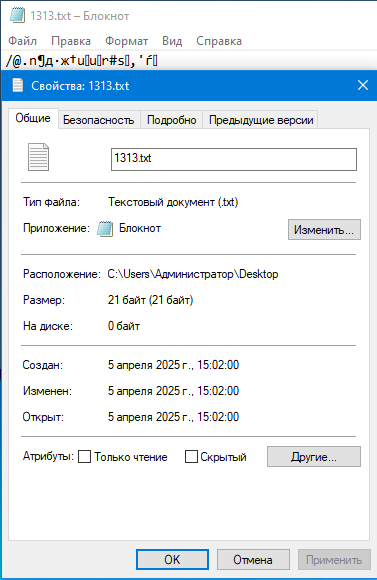


Рис. 3 – Зашифрованные данные

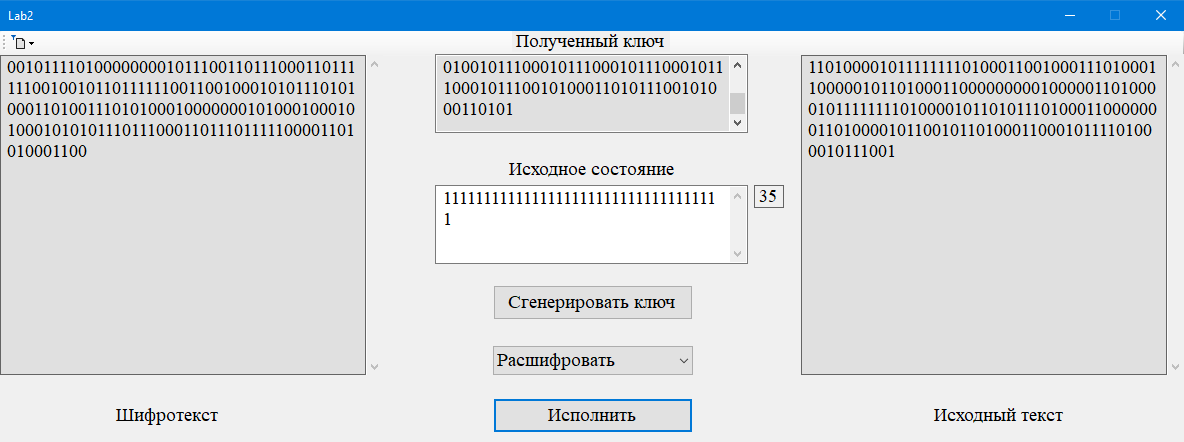


Рис. 4 – Дешифрование (после выполнения)

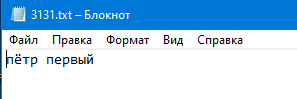


Рис. 5 – Результат дешифрования

Тест 2

**Состояние регистра:**

01010101010110011010011010101010110

**Ключ:** 01010101010110011010011010101010110111011101110000111010010001000100100111001001

...

10100111010110011000111111111011011011110010001111000001100110010010010011010000

**Исходный текст:**

00100101010100000100010001000110001011010011000100101110001101100000110100100101

...

00100000001000000010000000100000001000000010000000100000001000000000110100001010

**Зашифрованный текст:**

01110000000010011110001011101100111100001110110100010100011100100100010011101100

...

10000111011110011010111111011011010011110000001111100001101110010010100111011010

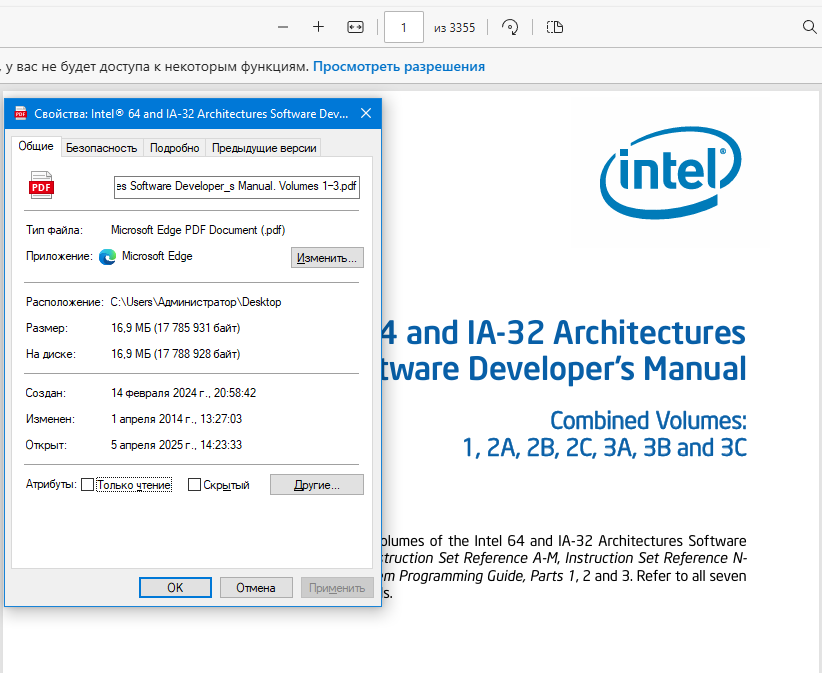


Рис. 6 – Исходные данные

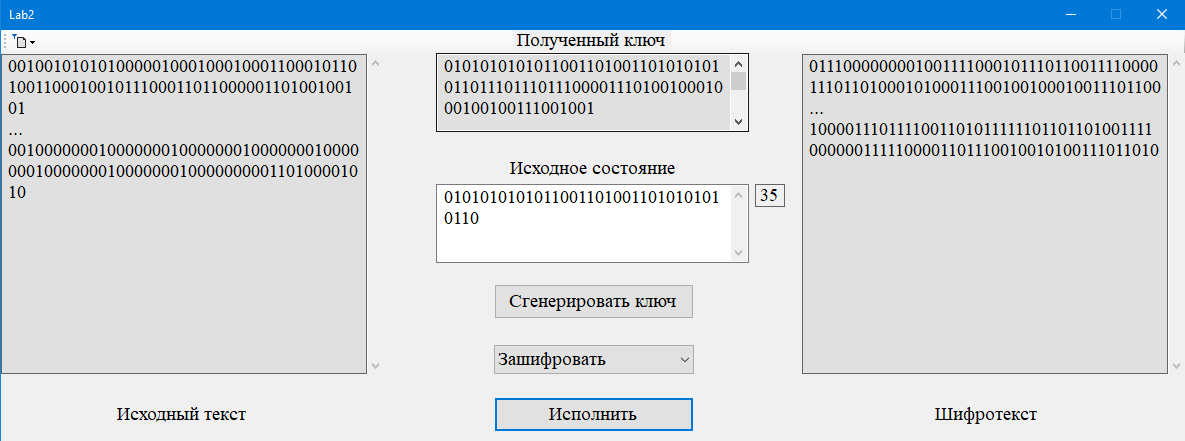


Рис. 7 – Шифрование (после выполнения)

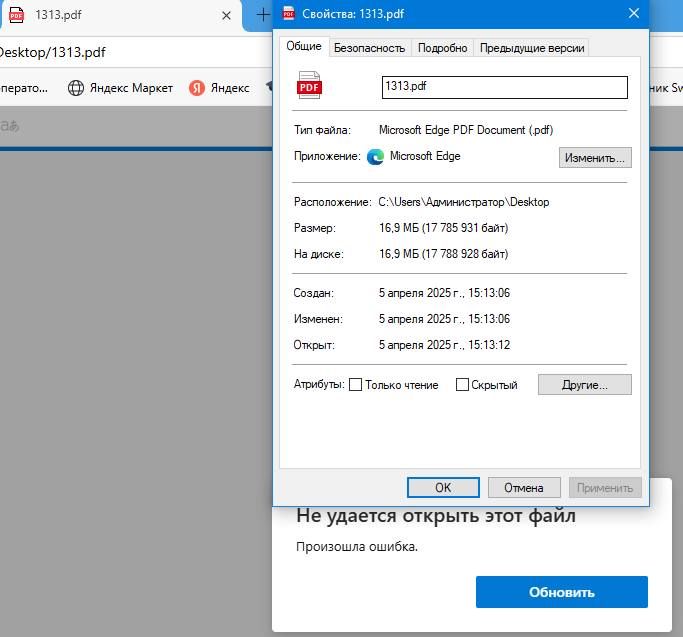


Рис. 8 – Зашифрованные данные

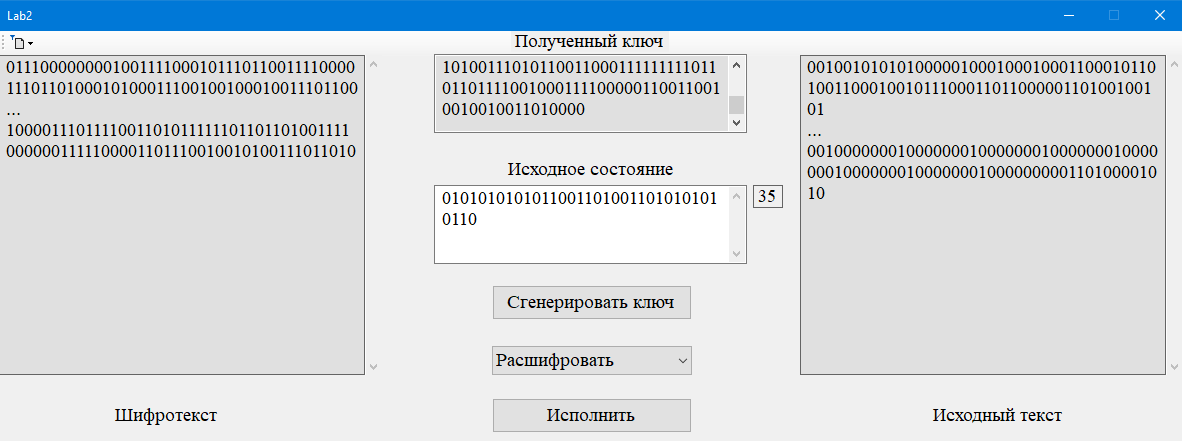


Рис. 9 – Дешифрование (после выполнения)

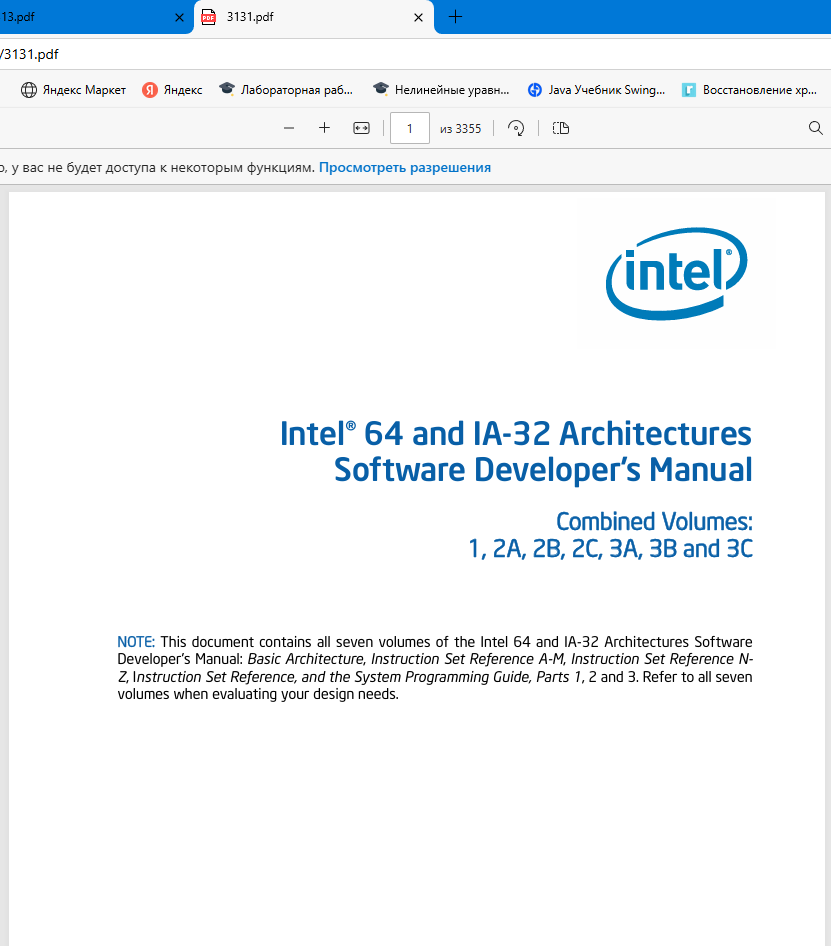


Рис. 10 – Результат дешифрования

Тест 3

**Состояние регистра:**

11111111111111111111000000000000000

**Ключ:** 11111111111111111111000000000000000110011001100110011000000000000000001111000011

...

10000000011100010100010010101100111010101010011111011111010001001011000100010000

**Исходный текст:**

00000000000000000000000000010100011001100111010001111001011100000111000101110100

...

01100110001101010011011100101110001101000011000100101110001100010011000000110000

**Зашифрованный текст:**

11111111111111111111000000010100011111111110110111100001011100000111001010110111

...

11100110010001000111001110000010110111101001011011110001011101011000000100100000

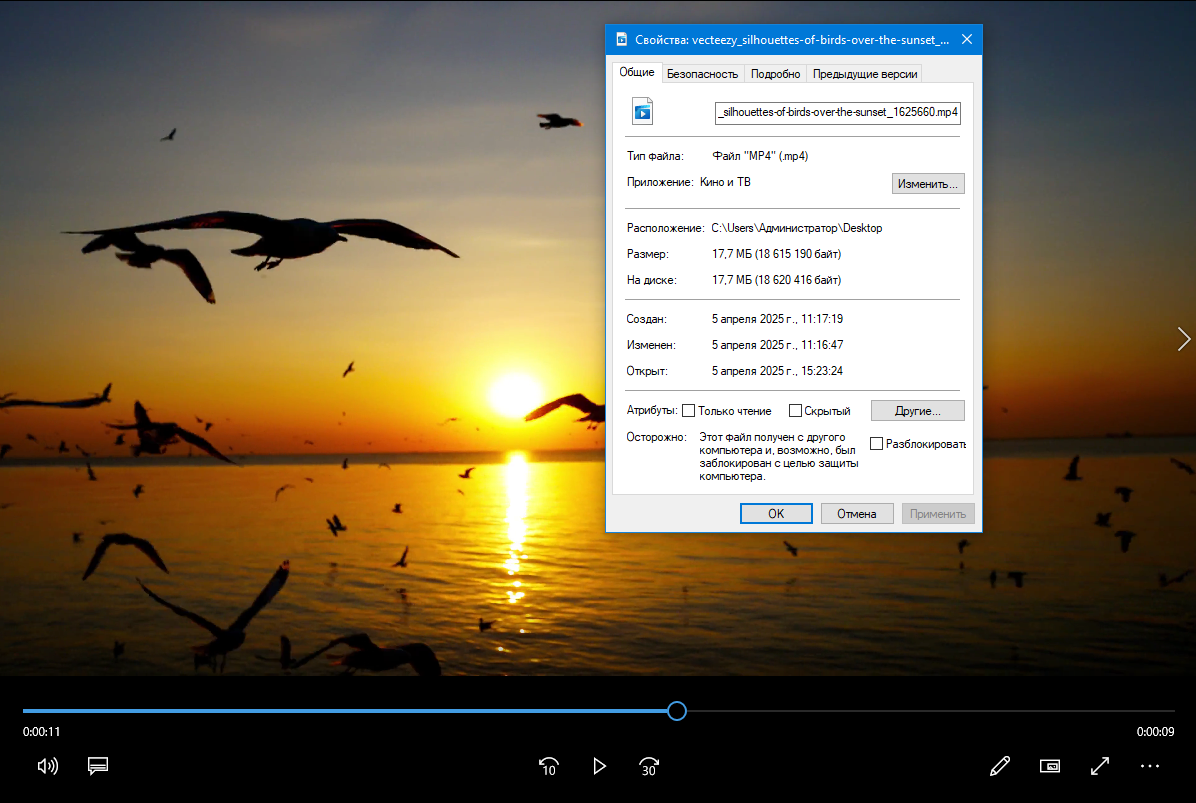


Рис. 11 – Исходные данные

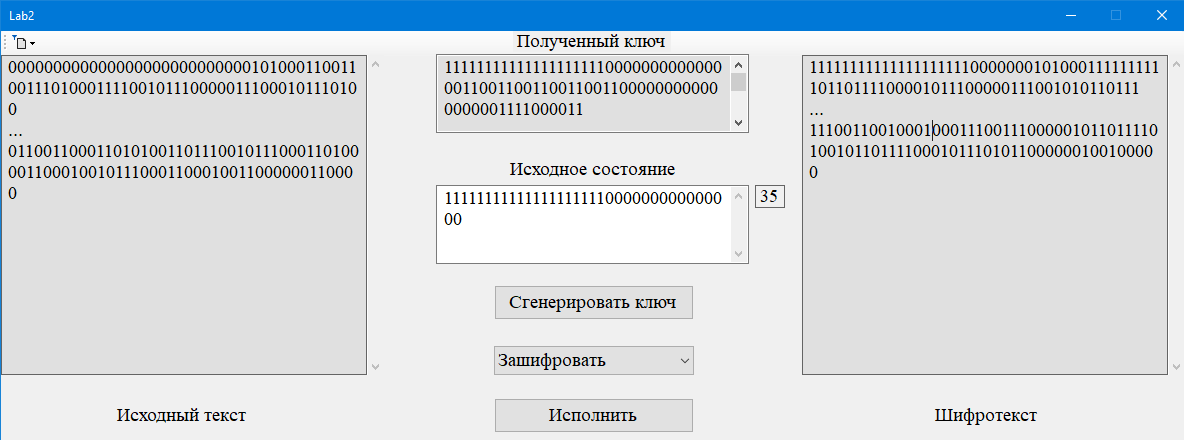


Рис. 12 – Шифрование (после выполнения)

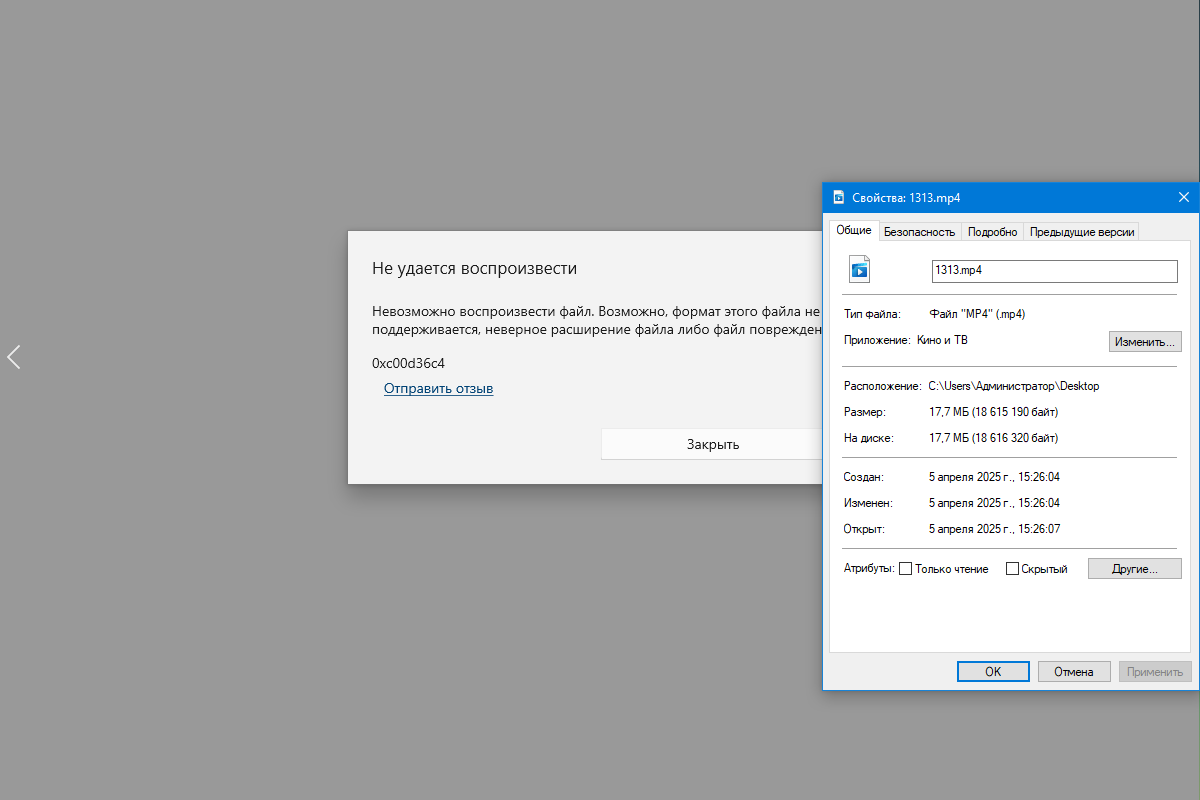


Рис. 13 – Зашифрованные данные

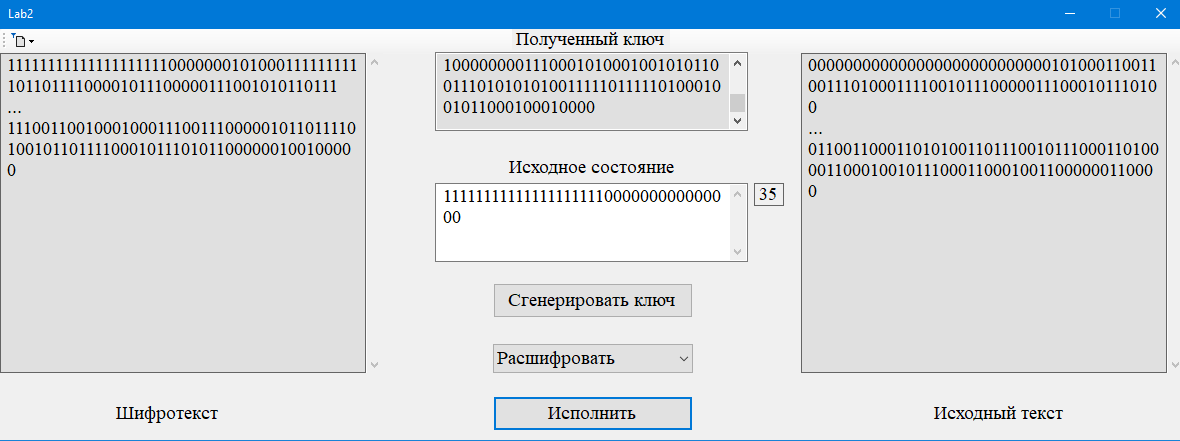


Рис. 14 – Дешифрование (после выполнения)

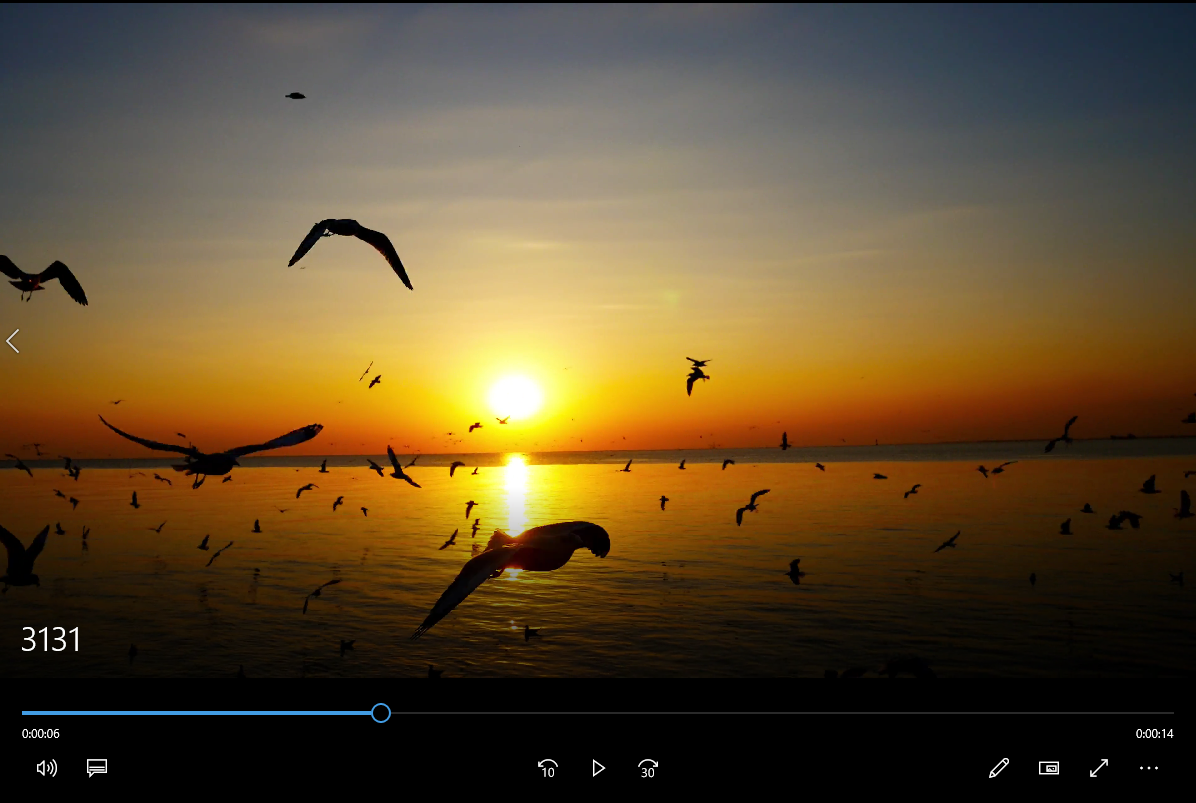


Рис. 15 – Результат дешифрования

Критические ситуации

**Состояние регистра:**

11111111111111111111000000000000000

**Ключ:**

-

**Исходный текст:**

- Ошибка, вызванная большим размером файла

**Зашифрованный текст:**

-

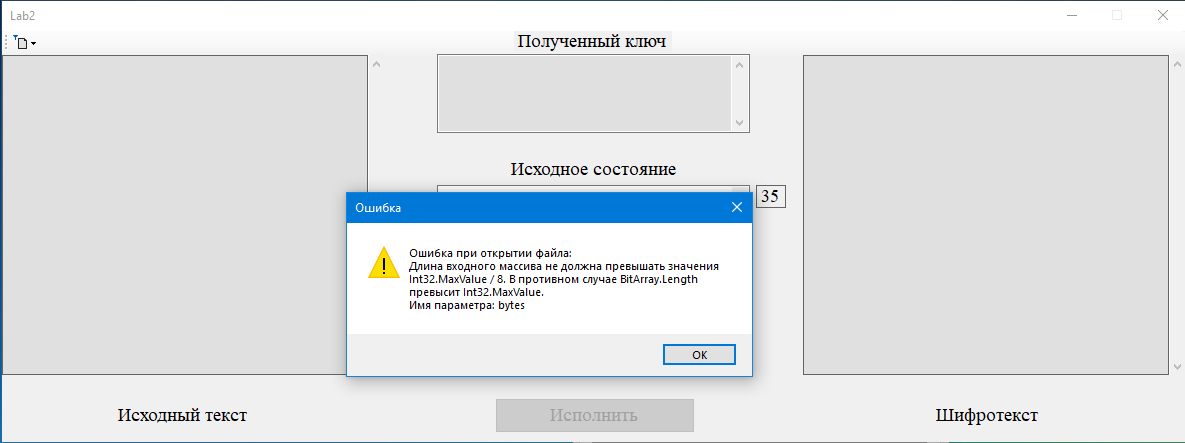


Рис. 16 – Критическая ситуация 1

**Состояние регистра:**

11111111111111111111000000000000000

**Ключ:**

11111111111111111111000000000000000110011001100110011000000000000000001111000011

...

10000000011100010100010010101100111010101010011111011111010001001011000100010000

**Исходный текст:**

00000000000000000000000000101000011001100010111010011110000011101000111000101110

...

01100110101011001110110001110100001011001000110001110100100011000000110000001100

**Зашифрованный текст:**

- Ошибка, вызванная сохранением пустого файла

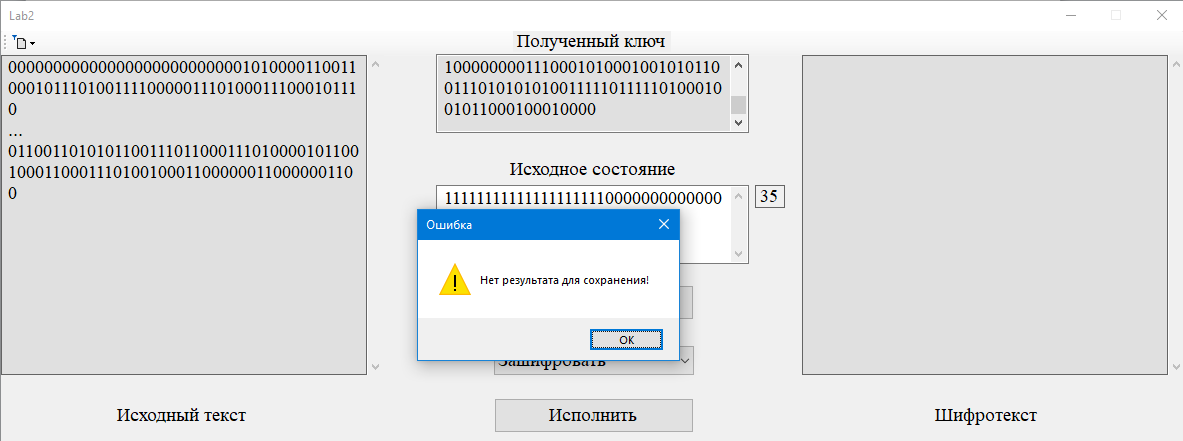


Рис. 17 – Критическая ситуация 2