УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №2

по предмету «Теория информации»

Вариант 9

Выполнил:

Ярохович Д. А.

Проверил:

Болтак С.В.

Группа 351002

Минск 2025

**Постановка задачи**

Имея текст и шифротекст определить длинну регистра и его начальное значение, вывести их вместе с характеристическим многочленом. Генератор ключа LSFR.

**Описание алгоритма**

Имея текст и его зашифрованную версию можно получить ключ шифрования. Ключ — последовательность сгенерированная используя LSFR. В данной ситуации ключ можно рассматривать как псевдобесконечное значение(как код Боуза-Чоудхури-Хоквингема).

**Алгоритм Берлекэмпа-Мэсси**

Алгоритм LSFR является линейной рекурентной функцией. Для поиска характеристического многочлена можно удобно использовать алгоритм Берлекэмпа-Мэсси.

Алгоритм Берлекэмпа-Мэсси — это эффективный метод нахождения минимального многочлена линейной рекуррентной последовательности над конечным полем.

1. Инициализация:

- C(x) = 1 (текущий многочлен)

- B(x) = 1 (предыдущий многочлен)

- L = 0 (текущая длина LFSR)

- m = 1 (номер итерации)

- b = 1 (предыдущая невязка)

2. Основной цикл:

- Вычислить невязку d ()

- Если d = 0, то C(x) пока корректен, перейти к следующему m.

- Если d != 0:

- Вычислить временный многочлен T(x) = C(x) - d \* (b^-1) \* x \* B(x).

- Если 2L <= m - 1, то:

- Обновить B(x) = C(x).

- Обновить L = m - L.

- Обновить b = d.

- Присвоить C(x) = T(x).

3. Возврат C(x) — минимального многочлена.

Пояснения:

- C(x) — искомый многочлен вида 1 + c\_1 x + c\_2 \* x^2 + ... + c\_L x^L.

- B(x) — предыдущий многочлен, который был корректен до текущего шага.

- L — текущая предполагаемая длина линейного регистра сдвига (LFSR).

- d — невязка, показывающая, насколько текущий C(x) ошибается на шаге m.

- Коррекция C(x) происходит только при ненулевой невязке.

Алгоритм эффективен и часто используется в декодерах Рида-Соломона для исправления ошибок.

**Тестирование**

Тестирование производится на данных полученных в результате выполнения лабораторных работ других учащихся.

Входные данные: 2 файла одинакового размера.

Выходные данные: длинна LSFR, коэфициенты характерестического многочлена, начальное состояние регистра.

Коэфициенты характерестического многочлена:

0100000001010000000000000000000000001 значат — 1 + x2 + x10 + x12 + x37.

Тест 1

Тестовая ситуация: проверка коректности результата работы программы при совподающем входном файле и выходном.

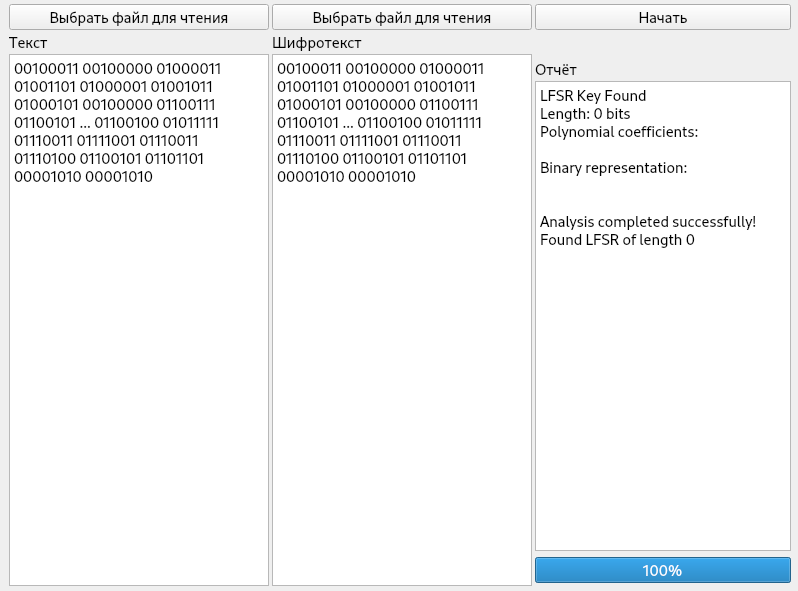
Данные шифрования:

Длинна регистра: 0.

Коэфициенты многочлена: .

Начальное значение регистра: .

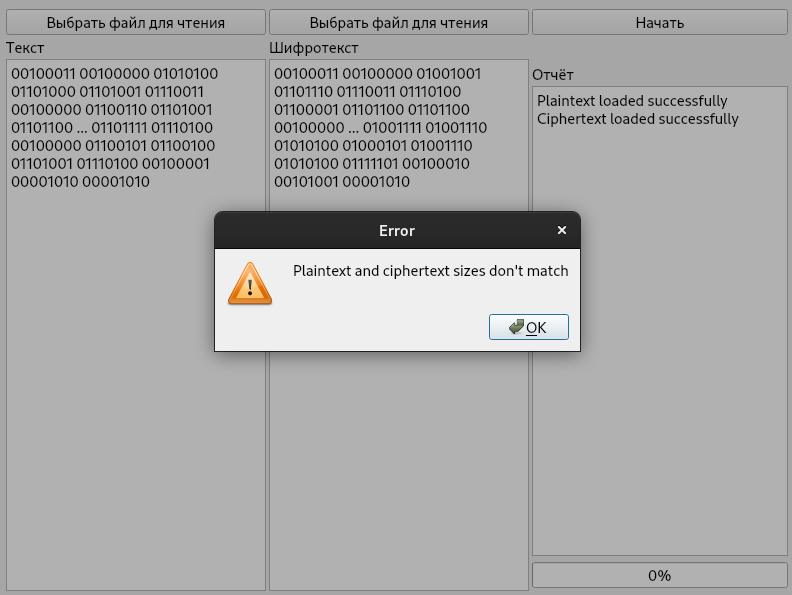
Описание: при добавлении одного и того же файла ключ состоит только из нулей, что определяет рекурентную зависимость пустой.



Тест 2

Тестовая ситуация: проверка коректности результата работы программы при файлах разной длины.

Описание: Оба файла должны быть одной длины, поэтому обработать файлы разной длины невозможно.



Тест 3

Тестовая ситуация: проверка коректности результата работы программы при корректных данных большого размера.

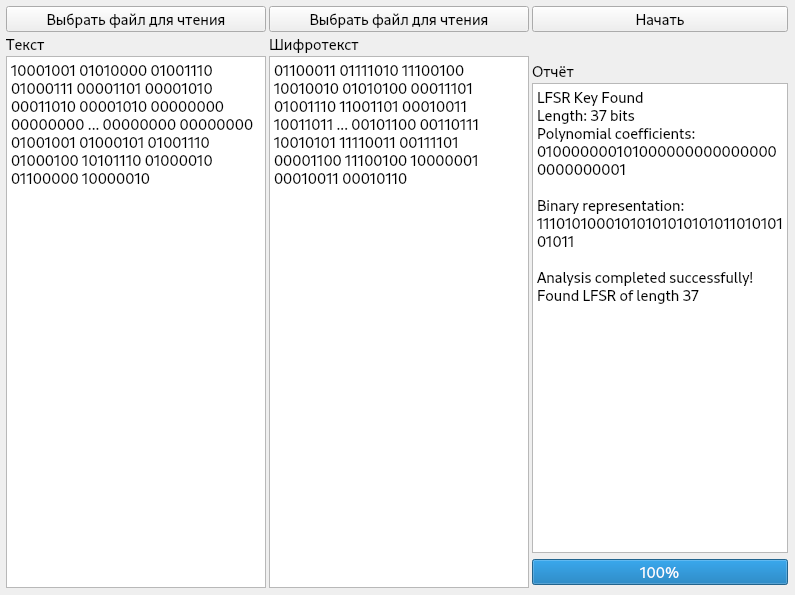
Данные шифрования:

Длинна регистра: 37.

Коэфициенты многочлена: 0100000001010000000000000000000000001.

Начальное значение регистра: 1110101000101010101010101101010101011.

Описание: параметры должны быть найдены быстро.



Тест 4

Тестовая ситуация: проверка коректности результата работы программы идентичных характерестических многочленах и отличающихся файлах и ином начальном значении регистра, по сравнению с тестом 3.

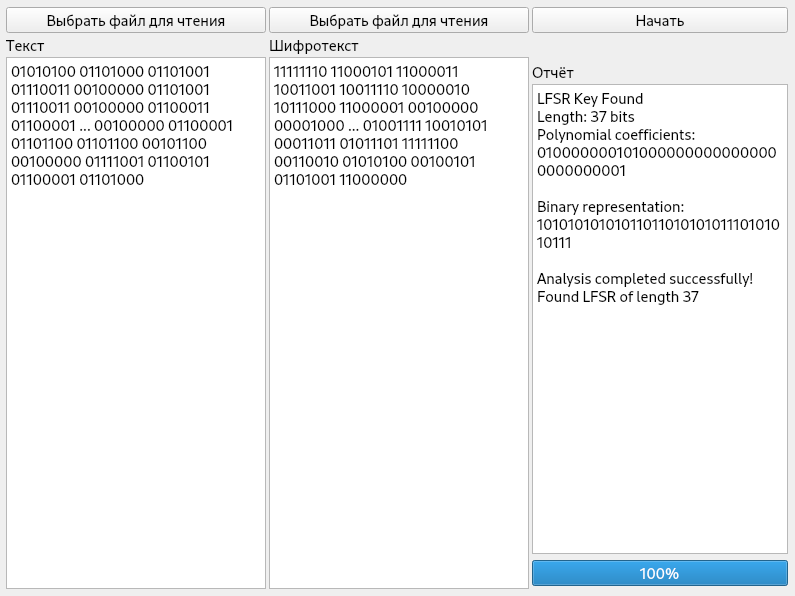
Данные шифрования:

Длинна регистра: 37.

Коэфициенты многочлена: 0100000001010000000000000000000000001.

Начальное значение регистра: 1010101010101101101010101110101010111.

Описание: должнен быть найден идентичный характерестический многочлен.



Тест 5

Тестовая ситуация: проверка коректности результата работы программы при корректных данных маленького размера.

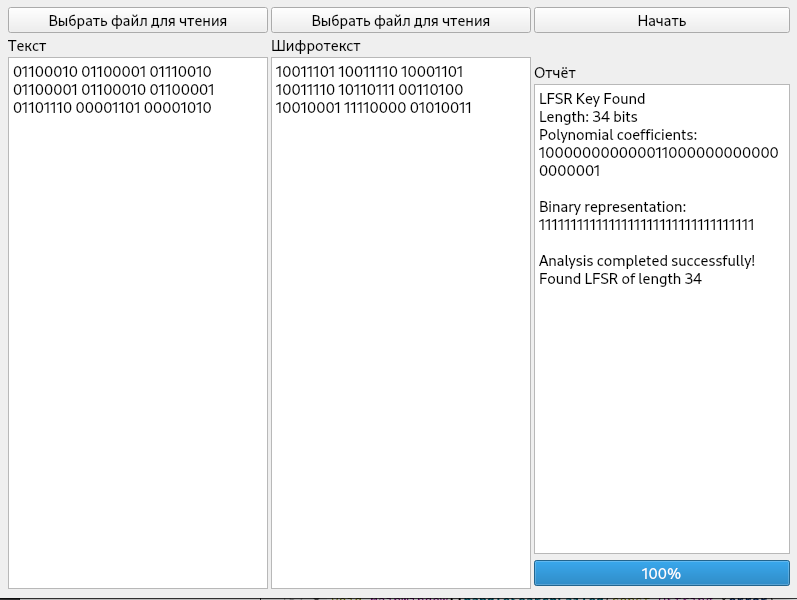
Данные шифрования:

Длинна регистра: 34.

Коэфициенты многочлена: 1000000000000110000000000000000001.

Начальное значение регистра: 1111111111111111111111111111111111.

Описание: минимальный объём данных необходимый для определения параметров регистра равен 2N+1 где N — длина регистра.



Тест 6

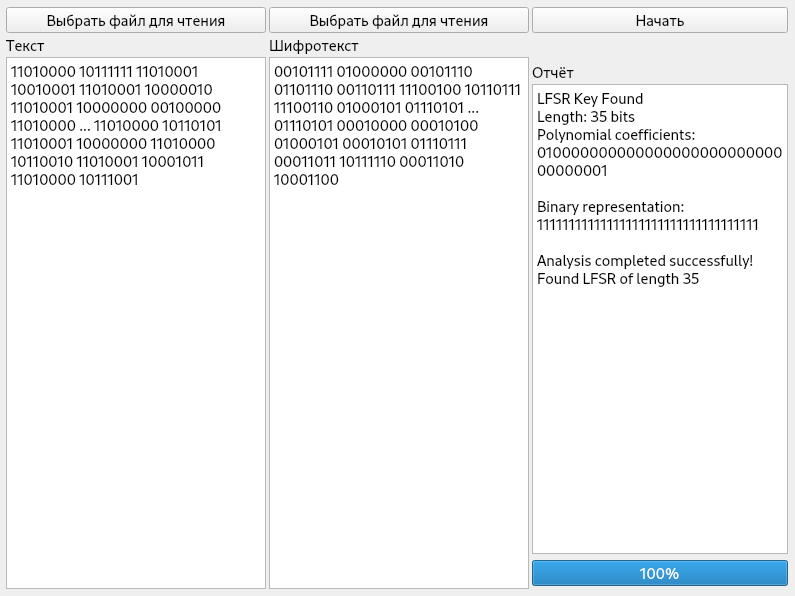
Тестовая ситуация: проверка коректности результата работы программы при корректных данных.

Данные шифрования:

Длинна регистра: 35.

Коэфициенты многочлена: 01000000000000000000000000000000001.

Начальное значение регистра: 11111111111111111111111111111111111.



Тест 7

Тестовая ситуация: проверка коректности результата работы программы при корректных данных.

Данные шифрования:

Длинна регистра: 280.

Коэфициенты многочлена:

0000000000000001000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001.

Начальное значение регистра:

1111111111111111111111111111111101100111011001100110011001100110101001101010010110100101101001011010010110100011101000111010001110100011010100111010110001010011101011001101001110110101110100111011010111010011100010011101001110001001110100111110100111010011111010011101001111101001.

