Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

Дисциплина: Теория информации (ТИ)

ОТЧЁТ

по практическому заданию №2

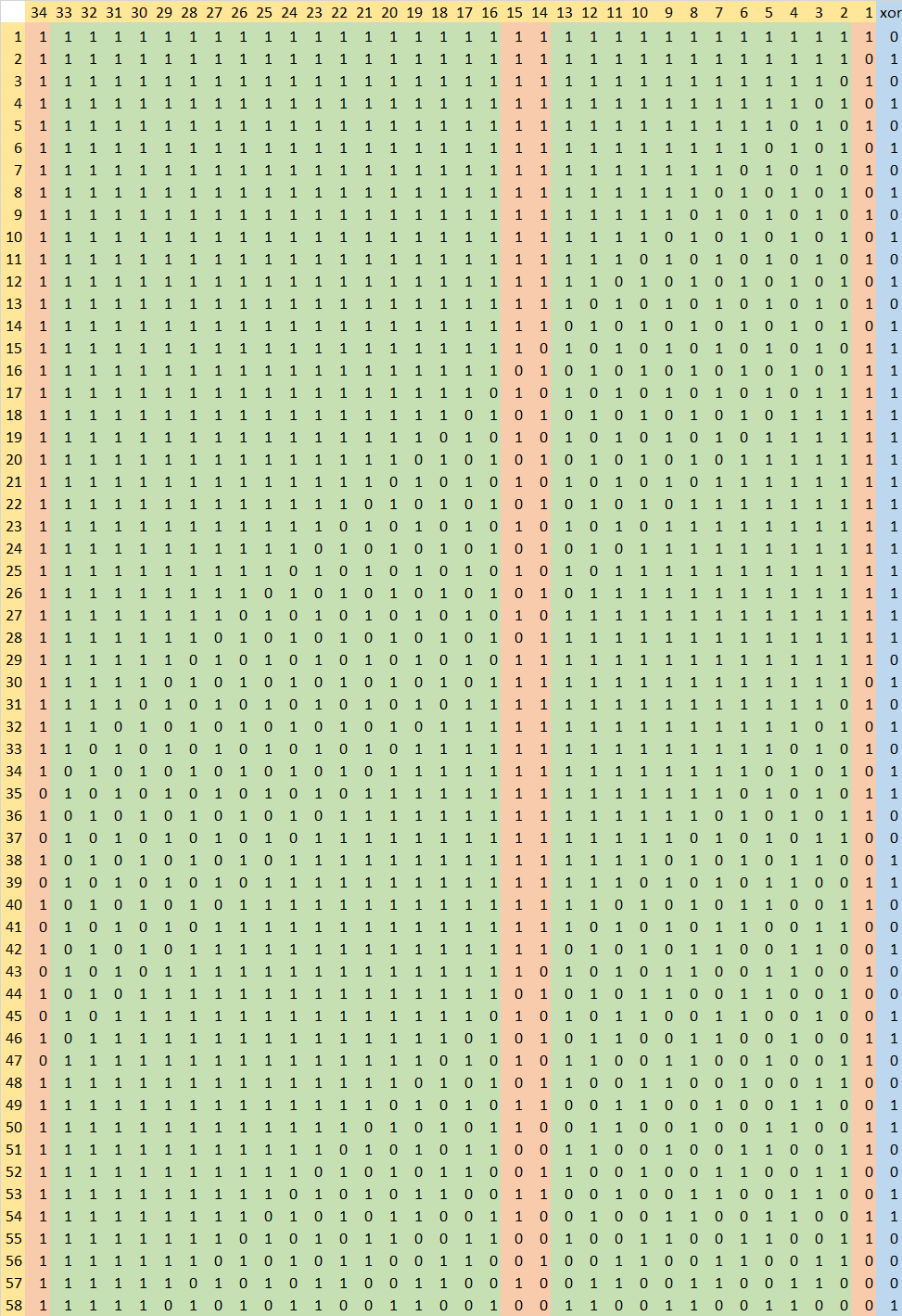
Тема работы: Потоковое шифрование

Выполнил

Проверил Болтак С.В.

Минск 2023

Примитивный многочлен согласно варианту: *x*34 + *x*15 +*x*14 + *x*+ 1.



## Описание

Выше приведена таблица состояний регистра. Основные характеристики:

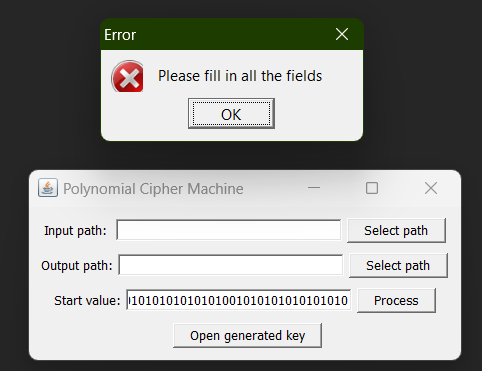
* Размерность регистра – 34.
* Строки – шаги/состояния регистра.
* Столбцы – полиномиальные степени.
* Первый столбец – ключевой поток.
* Последний столбец – результат функции обратной связи (xor выделенных битов)

## Тестирование ошибочных ситуаций

Программа не позволяет ввести начальное состояние регистра, если оно содержит не 34 символа или содержит что-то помимо «0» или «1».

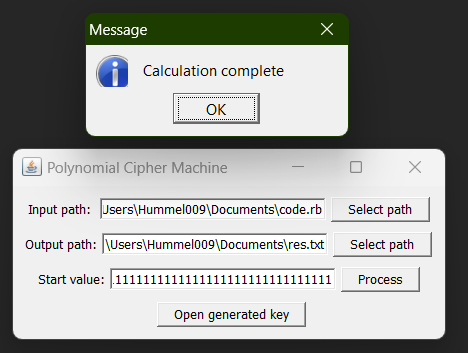
|  |  |
| --- | --- |
|  |  |

Также программа не позволяет начать обработку, если не выбраны файлы для шифрования.



## Тестирование валидных ситуаций

Файлы присутствуют и начальное состояние валидное. Шифрование успешно завершено.



Поскольку введённое состояние равнялось тридцати четырём единицам, сгенерированный ключ совпадает с ключевым потоком из таблицы на странице 2.

