Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное   
образовательное учреждение высшего образования

«Новгородский государственный университет имени Ярослава Мудрого»

ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ

Лабораторная Работа №2.   
Генераторы псевдослучайных величи

Отчет по лабораторной работе №2 по учебной дисциплине   
«Методы защиты информации»

по специальности 09.03.01 Информатика и вычислительная техника

|  |  |
| --- | --- |
|  | Руководитель  / Т. В. Жгун  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2024 г. |
|  | Студент группы 3091  / Р. А. Михайлов  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2024 г. |

Оглавление

[Линейный конгруэнтный генератор (](#_Toc182509155)*[LCG](#_Toc182509155)*[) 3](#_Toc182509155)

[Генератор псевдослучайных чисел (](#_Toc182509156)*[BBS)](#_Toc182509156)* [6](#_Toc182509156)

[Линейный рекуррентный генератор (](#_Toc182509157)*[LFSR](#_Toc182509157)*[) 9](#_Toc182509157)

[Приложение А 12](#_Toc182509158)

[Приложение Б 18](#_Toc182509159)

# Линейный конгруэнтный генератор (*LCG*)

Генератор определяется рекуррентным соотношением:

*X n + 1 = (a X n + c) mod m*

У последовательности, созданной с помощью *LCG* и определённой целыми параметрами *m, a, c* и *X0,* период максимален и равен числу *m,* когда выполняются следующие условия:

* *c* и *m* – взаимно просты:    
  (наибольший общий делитель *c* и *m* равен 1).
* *b = а - 1* – кратно любому простому числу, являющемуся делителем *m*, значением
* если *m* кратно 4, тогда *b* также кратно 4.

Популярным выбором *m* является степень двойки *2n.* Очень часто в качестве *m* выбирают одно из простых чисел Мерсенна .

В моей программе я установил следующие значения:

1. с = 1013904223
2. m = 2147483647 ()
3. a = 1664525
4. seed = 0

При помощи этого генератора я сгенерировал три битовых строки, из 50, 100 и 1000 битов. Битовые строки разделил на восьмибитные отрезки. Полученные восьмибитные значения перевел в десятичные для удобства отображения на гистограмме. Полученные гистограммы представлены ниже, полученные битовые строки, сгенерированные LCG генератором в Приложении А.1.

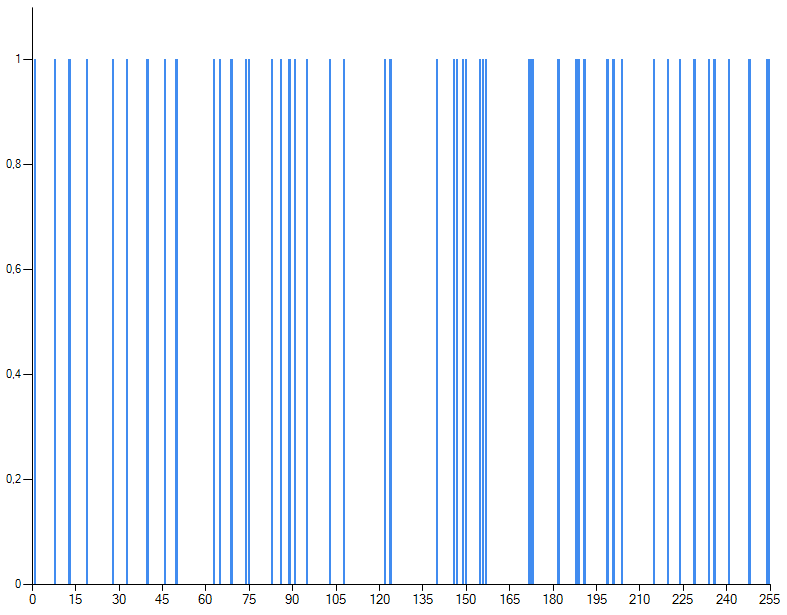


Рисунок 1 – Гистограмма 8-битных отрезков строки для 50 чисел LCG

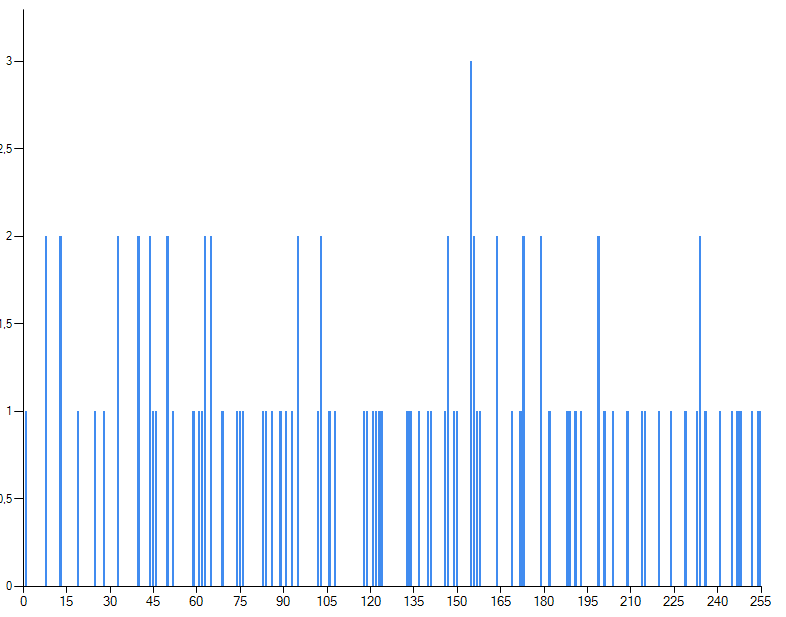


Рисунок 2 – Гистограмма 8-битных отрезков строки для 100 чисел LCG

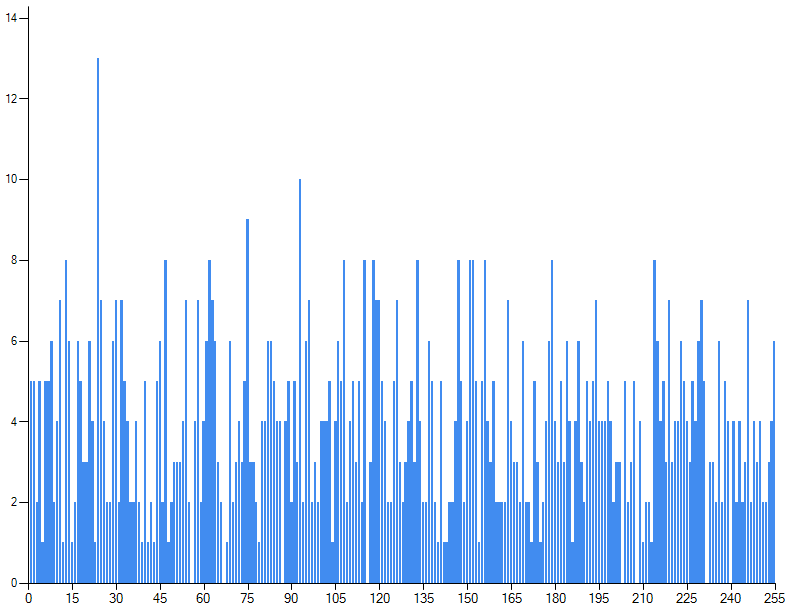


Рисунок 3 – Гистограмма 8-битных отрезков для 1000 чисел LCG

Генератор псевдослучайных чисел   
*BBS* (L. Blum, M. Blum, M. Shub) (генератор с квадратичным остатком)

1. Вначале выбираются два больших простых числа *p* и *q:*

p ≡ 3 mod 4, q ≡ 3 mod 4

1. Вычисляем число M = p q, называемое целым числом Блюма.
2. Выбирается случайное целое число *х*, взаимно простое с М.

(x, M) = 1

1. Вычисляем стартовое число генератора *х*0:

Псевдослучайная последовательность вырабатывается по правилу:

Результатом *n* - го шага является **один младший** **бит** числа *хn+1*. (Иногда в качестве результата принимают бит чётности). Для целей криптографии этот метод предложен в 1986 году.

В моей программе я установил следующие значения:

1. p = 3571
2. q = 3559
3. M = 12709189
4. seed = 255

При помощи этого генератора я сгенерировал три битовых строки, из 50, 100 и 1000 битов. Битовые строки разделил на восьмибитные отрезки. Полученные восьмибитные значения перевел в десятичные для удобства отображения на гистограмме. Полученные гистограммы представлены ниже, полученные битовые строки, сгенерированные BBS генератором в Приложении А.2.

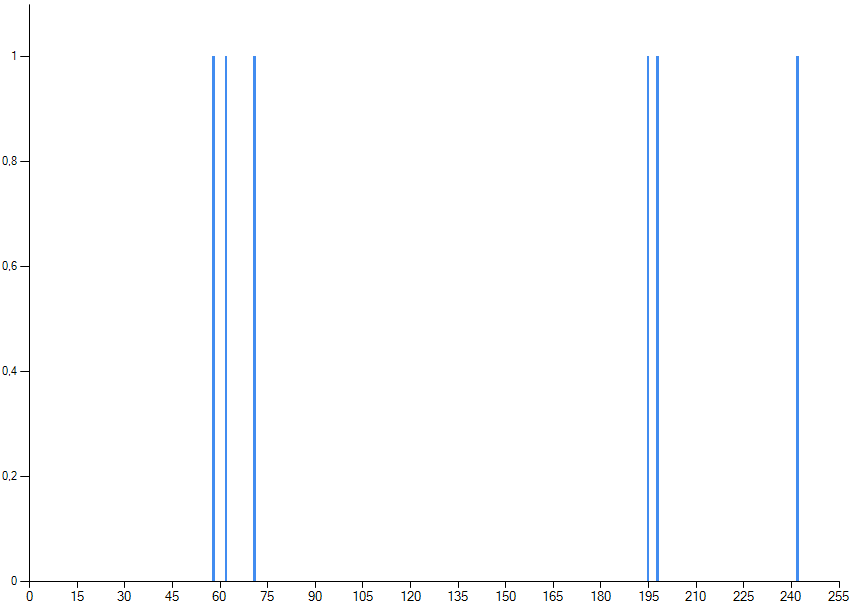


Рисунок 4 – Гистограмма 8-битных отрезков из 50-битной строки BBS

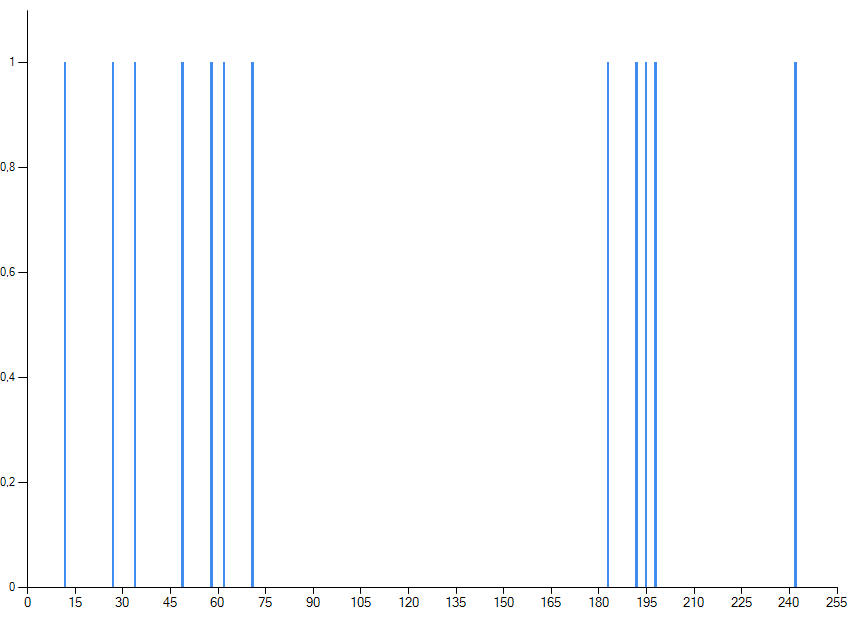


Рисунок 5 – Гистограмма 8-битных отрезков из 100-битной строки BBS

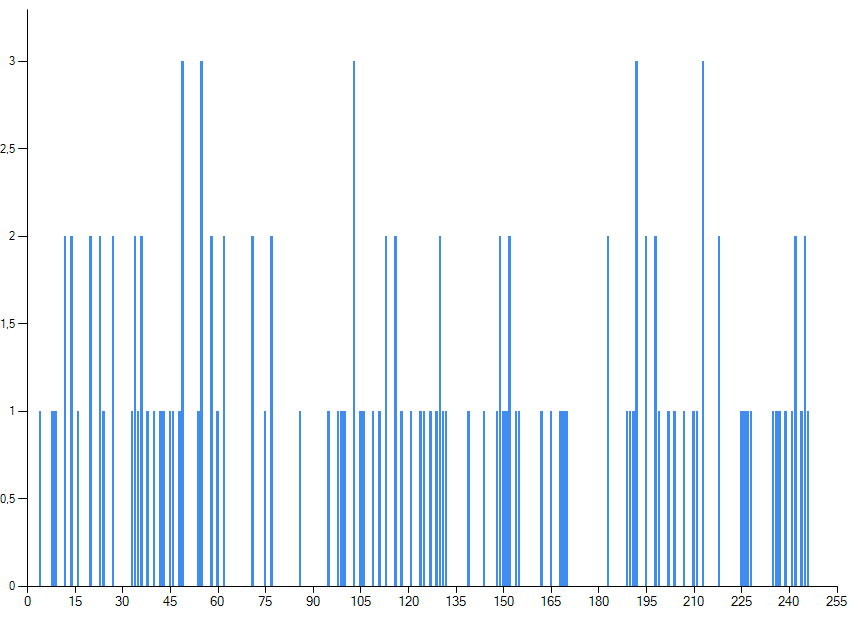


Рисунок 6 – Гистограмма 8-битных отрезков из 1000-битной строки BBS

# Линейный рекуррентный генератором (*LFSR*)

Работа генератора в поле моделируется уравнением

Генератор вырабатывает последовательность максимальной длины, если матрица А имеет вид: ,   
(an, an-1, …, a0) – коэффициенты неприводимого в поле многочлена. Соответствующий полином – x8 + x5 + x4 + x3 + 1.

В моей программе я установил следующие значения:

1. X = 181 (10110101)
2. A =

Такой выбор матрицы обусловлен тем, что при использовании матрицы из методических указаний, период генерации минимален (8 бит), а при использовании матрицы, представленной выше, период генерации больше (168 бит).

При помощи этого генератора я сгенерировал три битовых строки, из 50, 100 и 1000 битов. Битовые строки разделил на восьмибитные отрезки. Полученные восьмибитные значения перевел в десятичные для удобства отображения на гистограмме. Полученные гистограммы представлены ниже, полученные битовые строки, сгенерированные BBS генератором в Приложении А.3.

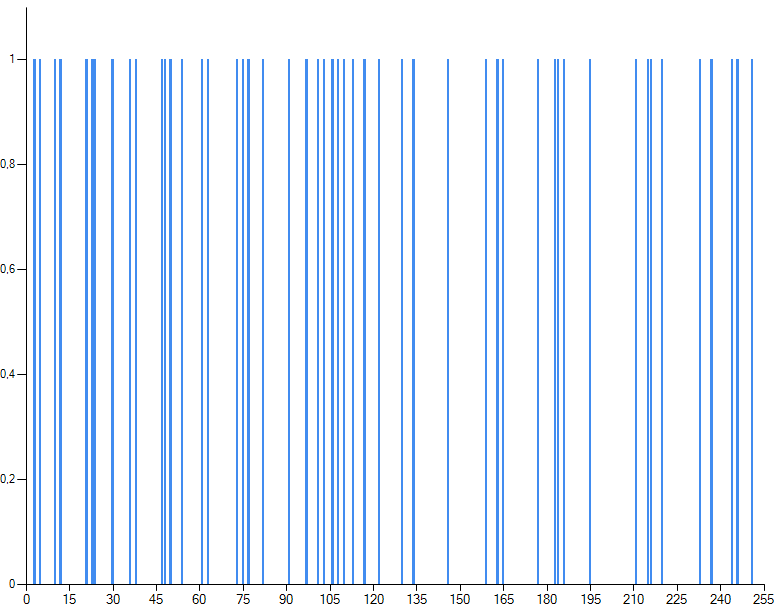


Рисунок 7 – Гистограмма 8-битных отрезков из 50 чисел LFSR

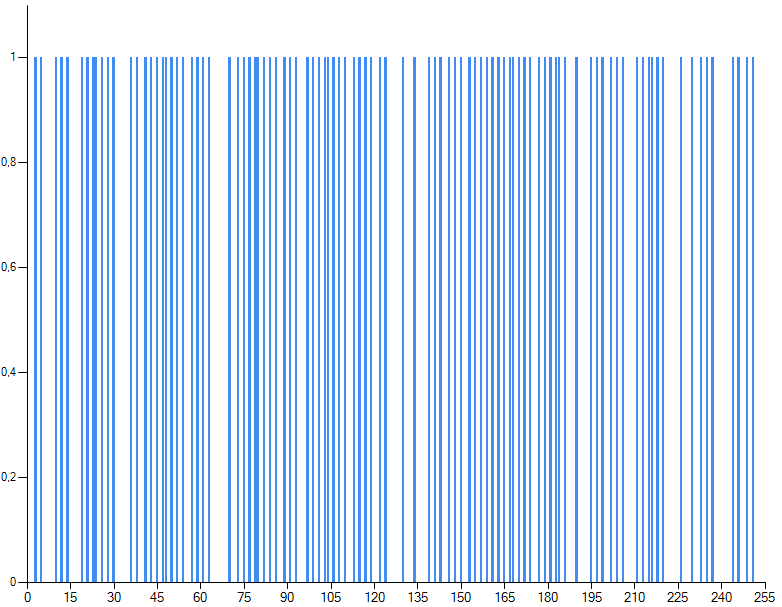


Рисунок 8 – Гистограмма 8-битных отрезков для 100 чисел LFSR

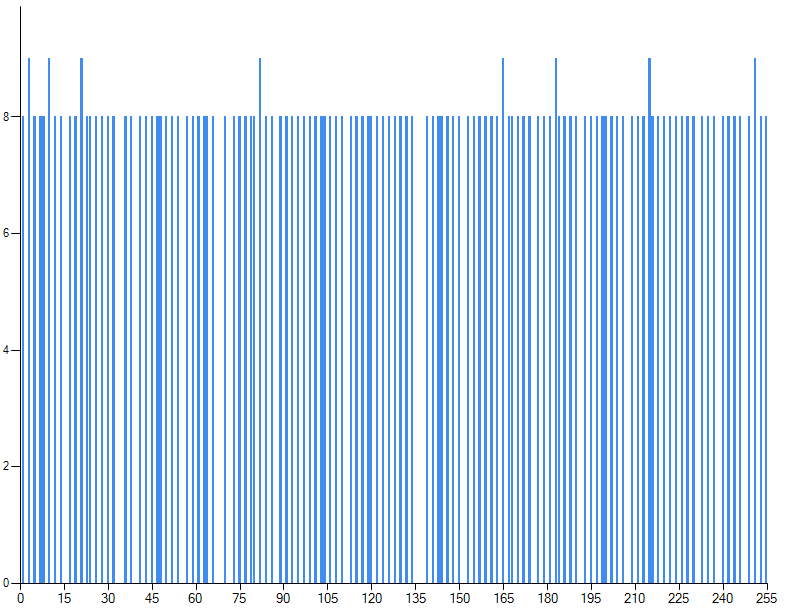


Рисунок 9 – Гистограмма 8-битных отрезков для 1000 чисел LFSR

# Приложение А

Приложение Б.1 LCG

Битовая строка для 50 8-битных чисел

0101111100110010111010100100000110101101001010000110011110011011001111111001001111010111010010100010000100001101000010001100011101111010100100101100100110010101111100011001110001001011001011101011011010011101010110011110010100000001011011001101110010001100011111001010110000011100110011001011110011101100010110111111111101010011100101101111111001000101111000001011111100010011010101101011110111111000

Битовая строка для 100 8-битных чисел

01011111001100101110101001000001101011010010100001100111100110110011111110010011110101110100101000100001000011010000100011000111011110101001001011001001100101011111000110011100010010110010111010110110100111010101100111100101000000010110110011011100100011000111110010101100000111001100110010111100111011000101101111111111010100111001011011111110010001011110000010111111000100110101011010111101111110001111011111101010010000011010110100101000011001111001101100111110100001100010110110101001111101011101000111111100001011001001101100111111100100111101011000111101011110011000010100100001000011010000100011000111011110111001111001100110100011011000100101010100101001001011001101110110010111010001100110100100101100110111011101101010110000010010110010011100010011000011101101011111001100101110100100110100

Битовая строка для 1000 8-битных чисел

01011111001100101110101001000001101011010010100001100111100110110011111110010011110101110100101000100001000011010000100011000111011110101001001011001001100101011111000110011100010010110010111010110110100111010101100111100101000000010110110011011100100011000111110010101100000111001100110010111100111011000101101111111111010100111001011011111110010001011110000010111111000100110101011010111101111110001111011111101010010000011010110100101000011001111001101100111110100001100010110110101001111101011101000111111100001011001001101100111111100100111101011000111101011110011000010100100001000011010000100011000111011110111001111001100110100011011000100101010100101001001011001101110110010111010001100110100100101100110111011101101010110000010010110010011100010011000011101101011111001100101110100100110100000000111000011100111010010100010111110110111001110001000101001110010111000010111110111110000011000001101010110100101000011001111001101100111111100100111101011000111110100001100010110110101001111101001100010001010011100101110000101111101110011101100101110100011001101001011100000000100000000000000101111100110011111101101101111010100110110011101101011000111110100001010010000000000000010111110011001111110110110111011001100000011000100101110000101111101111100000101111101000010010010010100010000100001101000010001100011101111011100111100110011010001101100010010101010010100011101001111101101001110001000111011101100001011000110110000101100011010111010010110010111111000010001110100101000101111100101010110000111000010110011111101100011001101110111101101101111010100110110011101101011000111110100001100010110110101001111101011101000111111101001110010100010011010100001000110010011001001101010010000000011110111011110111111011001001101001101101011001000010110000010100000110111100000010011110011000010100100000000000000110000001000000100111110111001100110110000111101110011000001101000010001100011101111010100100101100101010100001100011011000100001001000000001111011101111011111101100110111011001011110001001100100111001010110101111011111100100000100100101001110010011110011101101101001110101011001111001010000000001011111001100101110101001000010101110011100010101100000001111111001001111010110001111101000010100100000000000000101111100110011111101101101111010100101110000000001111111110010101010011111010111010001111111010011100101000101111000001100000000011111111100101010100111110100110001000101010010100011101001111101101001110001000111001100110010111100111011000101110000001011111011100111011001011101000110001001100000011000100110000001100010010111000010101110001011011010011100100010100101110101010100000110111100000010011110101001001011001010101000011000110110001001010101011011000101011101000110001001011100001011111011100111011001011101000110001001100000011000100110000001100010011000000110001001011100001010111000011100110010111100111011000101110000001100111110110001111011100110000011100001010101110001000111011101100001011000110101110100101100101111110000110100011011101110011101010101000001101111000000100111100110000100000101000110010001110011001101100001110111011001011001000111001100110111001010111000111110100010100110010010010000110100000001001001001111010110001111101000010100100000111111110101001110010110111111010011100101000101111000001011111100010010010010010001010101110000000100000011000011001111111000111110011100011010101100100110100110110100100001000001010001100011011001101000111010010101111100011001110001001011001011101011010110010001101111011111100011111000111110001111011111101011010011100101010110110001010111010001100010011000000101111000101001100001010011010100100000000111101110111101111110110010011010101100001000111010010100101000101001100010010110011110010100000001011011001101101101111110110001100110110111101001001101010001000100111101011110000111100001110111011010111100111111100010110110010110010110000001111011010110100010100111110110110111111011000101011000000100000010100000011111111101001100010110011111011011100010111000101110001011011110101010000000010110110011011011011111101100011001101110111101101101111010100110110011011100100110010100111000111110011100011010101100010101110100011000100110000001100010010111000010101110000111001100101111001110110001011011111111110101001110010110111111100100010111100000101111110001001101010110101111100000011010101110001101010001000100111100011011001101110010001011011011110000001001111001100001010010000000000000011000000011111110010011110101110100101000100010000110011010010010110011011101110110101111001111111000111110011000001110000101010111000100011101110110000101100011010111010010110010111111000011010001111111101100011110111001100000111000010110011111011011100010110111101010110000111000010101011100000000111100100010000110101011001001101001101101001000001100000110101011100011011000011110111001100000110100001000110010001000100001001000000001111011101111011111101100100110101011000001001011011010100011100111000110111011111100010010010010010001010101110001000111011101100101100100011100110011011100101010100000101111100100000100100101001110010011110011101101101001110101011001111001001111001110110110100111010101100111100101000000010110110011011011011111111101001000001010111000011100110010111100111010110100111101100011011001101000110110001001010101001010010010110100100000110000011010101101001010000110011110011010001100011101110010001011011011101111011011011101100110010010010101000000100111110111001100110110000111101110010100000000011000000011111110010010110010101010001010011001001001000011010000000100100100111101011000111110100001010010000100001101000010001100100010000111001110110101111000100101010000001001111101110011001101100001110111011001011001011000000111101101011010011011010110010000101011110100001010111001110001000101010010100100101100110111011001011101000110011010010010110011011101110110101111001110110101100011110101111000011101110110101011000001001011001001110001001100001111000110101111001111111000101101100101100101100000011110110001011011111111100100010111100000110000000010000011111111010100101000101001100001010011010100100100010100011001000111001100110110000111101110010100000001011011001101101101111110110001100110110111101001001101010001000100111101011110011000010000010011010101101011111000000101101000001000000011011111101100110111011001011101000110011010010111000001001011011010100011100111000110101011001001101010110000100011101001010010100010100110001001011010111100011001110001001011001011111100001101000111111110100001000100111101011110000111011101101010110000100011101001010010100010010101010110110001010111000000101111101111100000110000011010101110001101010001000100111100011011001101101101111111110100110001011001111110110001010110000000111111100100111101011101001011001011111100001000111001010001011110000111001101110010011001010011100011111001110001101110111111000100100100101000100010000110011010010111000001001011001001110001001011001011111100001101000111111110100001001001001010001000100001100110100100101101001000001100000111101110101101000111111100001011001001110001001100001111000110110011011011011111101100011001101110111101101101110110011001001001010100000010011111011100100010101010000010111110010000010010010100111001001111001110110110100111100110010110000000110111111011001101110110010111010001100010010111000010111110111110000010111110100001000100111101011110000111100001111000011101110110101111001111111000111110011000001110000101010111000000010000001011111100001000111010010100010111110110111001110001010110000001000000100111110111001100110110000111101110011000001101000010011101010100110001110111011001100100100101010000011010110100101000011001111001101100111110100001010010000100001101000010011101010000100011001001110101101111111111010100111001011011111110010001101110111001110101010100010111110110111000101110001011011110101010000000100111101010010001101111001110110001011011111111110101001010001010011000100101101011110001100111000100101100101111110000100011101001010010100010010101010110110000010100000110111100000011100001100010110110101001

Приложение Б.2 BBS

Битовая строка из 50

110000110111110001001111111000100110001101011100001

Битовая строка из 100 битов

11000011011111000100111111100010011000110101110000110000111011010100010000000011100011001101100011101

Битовая строка из 1000 битов

11000011011111000100111111100010011000110101110000110000111011010100010000000011100011001101100011101100010110110100011001011001001000010100010101010100000110011011001011010100011100001000000101101001000011001110011011101001001010001010111100110111010000011100011110001110110000011110001101101111010101011010100110000111010000010010011010111110100001001011010010001110001001001110100000011001111010000010111011000110111110100111010010001111111100110010111000010000011100000010011111010001011011100011001100010100111111100111110100101111100100001110110001010110001010011001010111010010110010110000100001001011000000110010000011000100000110001101100110011110000010010101001101101010101111010011110011111101001001001010101111110111001010001001011000111110111001100001010111100110110101111010100110101011101101101010101110001100101011111010010101100100101100100110110001000111111101101011011111000011011111000100111111100010011000110101110000110000111011010100010000000011100011001101100011101100010110110

Приложение Б.3 LFSR

Битовая строка для 50 8-битных чисел

0000001111111011000010100001010111010111010100101010010110110111100100100010010001001001011011101101110010111000011100010001111000111101100001100000110000011000001100000110000100111111100000100000010111110110111011010010011001001101011001110011001001100101001101100110110011011000101100011001111111000011011110101111010011101001001011111010001110111010011101010001011111010011010110110100101101101010

Битовая строка для 100 8-битных чисел

00000011111110110000101000010101110101110101001010100101101101111001001000100100010010010110111011011100101110000111000100011110001111011000011000001100000110000011000001100001001111111000001000000101111101101110110100100110010011010110011100110010011001010011011001101100110110001011000110011111110000110111101011110100111010010010111110100011101110100111010100010111110100110101101101001011011010101101010101010110101011000101100101001111011000110011101110001011111010110010101110101010010101001010100001010000101000011011111001111100111110010000111000011100001110011000111111100010110001010111011100010011110110101011010110010110001011011010011110110011100110111100101010010100001010011010111001011101010001101000110111100110110011001001100111001110100111011100011101110011000110100011010001101000

Битовая строка для 1000 8-битных чисел

00000011111110110000101000010101110101110101001010100101101101111001001000100100010010010110111011011100101110000111000100011110001111011000011000001100000110000011000001100001001111111000001000000101111101101110110100100110010011010110011100110010011001010011011001101100110110001011000110011111110000110111101011110100111010010010111110100011101110100111010100010111110100110101101101001011011010101101010101010110101011000101100101001111011000110011101110001011111010110010101110101010010101001010100001010000101000011011111001111100111110010000111000011100001110011000111111100010110001010111011100010011110110101011010110010110001011011010011110110011100110111100101010010100001010011010111001011101010001101000110111100110110011001001100111001110100111011100011101110011000110100011010001101000110100010101111101000010100001000000100000010001110111101011110001111000111100001110000011000001011111101111110100000111111100101110010011001000100100000010000001000000100000000000000111111111000000111111101100001010000101011101011101010010101001011011011110010010001001000100100101101110110111001011100001110001000111100011110110000110000011000001100000110000011000010011111110000010000001011111011011101101001001100100110101100111001100100110010100110110011011001101100010110001100111111100001101111010111101001110100100101111101000111011101001110101000101111101001101011011010010110110101011010101010101101010110001011001010011110110001100111011100010111110101100101011101010100101010010101000010100001010000110111110011111001111100100001110000111000011100110001111111000101100010101110111000100111101101010110101100101100010110110100111101100111001101111001010100101000010100110101110010111010100011010001101111001101100110010011001110011101001110111000111011100110001101000110100011010001101000101011111010000101000010000001000000100011101111010111100011110001111000011100000110000010111111011111101000001111111001011100100110010001001000000100000010000001000000000000001111111110000001111111011000010100001010111010111010100101010010110110111100100100010010001001001011011101101110010111000011100010001111000111101100001100000110000011000001100000110000100111111100000100000010111110110111011010010011001001101011001110011001001100101001101100110110011011000101100011001111111000011011110101111010011101001001011111010001110111010011101010001011111010011010110110100101101101010110101010101011010101100010110010100111101100011001110111000101111101011001010111010101001010100101010000101000010100001101111100111110011111001000011100001110000111001100011111110001011000101011101110001001111011010101101011001011000101101101001111011001110011011110010101001010000101001101011100101110101000110100011011110011011001100100110011100111010011101110001110111001100011010001101000110100011010001010111110100001010000100000010000001000111011110101111000111100011110000111000001100000101111110111111010000011111110010111001001100100010010000001000000100000010000000000000011111111100000011111110110000101000010101110101110101001010100101101101111001001000100100010010010110111011011100101110000111000100011110001111011000011000001100000110000011000001100001001111111000001000000101111101101110110100100110010011010110011100110010011001010011011001101100110110001011000110011111110000110111101011110100111010010010111110100011101110100111010100010111110100110101101101001011011010101101010101010110101011000101100101001111011000110011101110001011111010110010101110101010010101001010100001010000101000011011111001111100111110010000111000011100001110011000111111100010110001010111011100010011110110101011010110010110001011011010011110110011100110111100101010010100001010011010111001011101010001101000110111100110110011001001100111001110100111011100011101110011000110100011010001101000110100010101111101000010100001000000100000010001110111101011110001111000111100001110000011000001011111101111110100000111111100101110010011001000100100000010000001000000100000000000000111111111000000111111101100001010000101011101011101010010101001011011011110010010001001000100100101101110110111001011100001110001000111100011110110000110000011000001100000110000011000010011111110000010000001011111011011101101001001100100110101100111001100100110010100110110011011001101100010110001100111111100001101111010111101001110100100101111101000111011101001110101000101111101001101011011010010110110101011010101010101101010110001011001010011110110001100111011100010111110101100101011101010100101010010101000010100001010000110111110011111001111100100001110000111000011100110001111111000101100010101110111000100111101101010110101100101100010110110100111101100111001101111001010100101000010100110101110010111010100011010001101111001101100110010011001110011101001110111000111011100110001101000110100011010001101000101011111010000101000010000001000000100011101111010111100011110001111000011100000110000010111111011111101000001111111001011100100110010001001000000100000010000001000000000000001111111110000001111111011000010100001010111010111010100101010010110110111100100100010010001001001011011101101110010111000011100010001111000111101100001100000110000011000001100000110000100111111100000100000010111110110111011010010011001001101011001110011001001100101001101100110110011011000101100011001111111000011011110101111010011101001001011111010001110111010011101010001011111010011010110110100101101101010110101010101011010101100010110010100111101100011001110111000101111101011001010111010101001010100101010000101000010100001101111100111110011111001000011100001110000111001100011111110001011000101011101110001001111011010101101011001011000101101101001111011001110011011110010101001010000101001101011100101110101000110100011011110011011001100100110011100111010011101110001110111001100011010001101000110100011010001010111110100001010000100000010000001000111011110101111000111100011110000111000001100000101111110111111010000011111110010111001001100100010010000001000000100000010000000000000011111111100000011111110110000101000010101110101110101001010100101101101111001001000100100010010010110111011011100101110000111000100011110001111011000011000001100000110000011000001100001001111111000001000000101111101101110110100100110010011010110011100110010011001010011011001101100110110001011000110011111110000110111101011110100111010010010111110100011101110100111010100010111110100110101101101001011011010101101010101010110101011000101100101001111011000110011101110001011111010110010101110101010010101001010100001010000101000011011111001111100111110010000111000011100001110011000111111100010110001010111011100010011110110101011010110010110001011011010011110110011100110111100101010010100001010011010111001011101010001101000110111100110110011001001100111001110100111011100011101110011000110100011010001101000110100010101111101000010100001000000100000010001110111101011110001111000111100001110000011000001011111101111110100000111111100101110010011001000100100000010000001000000100000000000000111111111000000111111101100001010000101011101011101010010101001011011011110010010001001000100100101101110110111001011100001110001000111100011110110000110000011000001100000110000011000010011111110000010000001011111011011101101001001100100110101100111001100100110010100110110011011001101100010110001100111111100001101111010111101001110100100101111101000111011101001110101000101111101001101011011010010110110101011010101010101101010110001011001010011110110001100111011100010111110101100101011101010100101010010101000010100001010000110111110011111001111100100001110000111000011100110001111111000101100010101110111000100111101101010110101100101100010110110100111101100111001101111001010100101000010100110101110010111010100011010001101111001101100110010011001110011101001110111000111011100110001101000110100011010001101000101011111010000101000010000001000000100011101111010111100011110001111000011100000110000010111111011111101000001111111001011100100110010001001000000100000010000001000000000000001111111110000001111111011000010100001010111010111010100101010010110110111

# Приложение Б

Листинг файла LCG.h

#pragma once

#include <vector>

#include <limits>

#include <stdexcept>

#define MAX std::numeric\_limits<uint>::max()

typedef unsigned int uint;

class LCG {

public:

LCG() {}

uint8\_t generate() {

return last\_generated = (a \* last\_generated + c) % m;

}

private:

bool is\_coprime(uint a, uint b) {

while (b != 0) {

uint temp = b;

b = a % b;

a = temp;

}

return a == 1;

}

uint seed = 0;

uint m = 2147483647; // Число Мерсена 2^31 - 1 (2^p - 1)

uint a = 1664525;

uint c = 1013904223;

uint last\_generated = seed % m;

};

Листинг файла BBS.h

#pragma once

#include <vector>

#include <limits>

#include <stdexcept>

class BBS {

public:

BBS() : seed(255), p(3571), q(3559), M(p\* q), last\_generated((seed\* seed) % M) {

if (!is\_coprime(M, seed))

throw std::invalid\_argument("M и seed не взаимнопростые\n");

}

bool generate() {

last\_generated = (last\_generated \* last\_generated) % M;

return std::bitset<1>(last\_generated)[0];

}

private:

bool is\_coprime(size\_t a, size\_t b) {

while (b != 0) {

size\_t temp = b;

b = a % b;

a = temp;

}

return a == 1;

}

size\_t seed;

size\_t p;

size\_t q;

size\_t M;

size\_t last\_generated;

};

Листинг файла LFSR.h

#pragma once

class LFSR {

public:

LFSR() : last\_generated(181) {}

std::bitset<8> generate() {

std::bitset<8> res;

for (int i = 0; i < 8; i++) {

bool feedback = last\_generated[0];

for (int j = 1; j < 8; j++) {

feedback ^= (matrix[i][j] ? last\_generated[j] : 0);

}

res[i] = feedback;

}

last\_generated = res;

return last\_generated;

}

private:

std::bitset<8> last\_generated;

std::vector<std::vector<bool>> matrix = {

{0, 0, 1, 1, 1, 0, 0, 1},

{1, 0, 0, 0, 0, 0, 0, 0},

{0, 1, 0, 0, 0, 0, 0, 0},

{0, 0, 1, 0, 0, 0, 0, 0},

{0, 0, 0, 1, 0, 0, 0, 0},

{0, 0, 0, 0, 1, 0, 0, 0},

{0, 0, 0, 0, 0, 1, 0, 0},

{0, 0, 0, 0, 0, 0, 1, 0}

};

};

Листинг файла MZI\_2.cpp

#include <iostream>

#include <fstream>

#include <conio.h>

#include <string>

#include <bitset>

#include "LCG.h"

#include "BBS.h"

#include "LFSR.h"

typedef unsigned int uint;

int LCG\_init();

int BBS\_init();

int LFSR\_init();

int main()

{

setlocale(0, "");

unsigned char ch = 0;

while (ch != '4') {

system("cls");

std::cout << "МЕНЮ\n\n1. LCG\n2. BBS\n3. LFSR\n4. Выход\n>> ";

ch = \_getch();

if (ch < '4') {

switch (ch) {

case '1': LCG\_init(); break;

case '2': BBS\_init(); break;

case '3': LFSR\_init(); break;

}

}

}

return 0;

}

int LCG\_init() {

system("cls");

uint n = 0, seed = 0, a = 0, c = 0, m = 0;

std::cout << "LCG generator\n\nВведите требуемое количество 8-битных чисел\n>> ";

std::cin >> n;

std::ofstream out("generated\_LCG.bin", std::ios::binary);

if (!out.is\_open()) {

std::cout << "File was not opened\n";

return 1;

}

LCG LCG;

std::vector<uint8\_t> decimal;

std::bitset<8> b;

system("cls");

std::cout << "Сгенерированная LCG последовательность\n\nВ виде битовой строки:\n";

for (int i = 0; i < n; i++) {

decimal.push\_back(LCG.generate());

std::cout << std::bitset<8>(decimal.back());

out.write(reinterpret\_cast<const char\*>(&decimal.back()), sizeof(uint8\_t));

}

std::cout << std::endl << "\nВ виде 8-битных чисел:\n";

for (int i = 0; i < decimal.size(); i++) {

std::cout << (int)decimal[i] << " ";

}

std::cout << std::endl << std::endl;

out.close();

system("pause");

return 0;

}

int BBS\_init() {

system("cls");

uint n = 0, seed = 0, a = 0, c = 0, m = 0;

std::cout << "BBS generator\n\nВведите требуемое количество битов\n>> ";

std::cin >> n;

std::ofstream out("generated\_BBS.bin", std::ios::binary);

if (!out.is\_open()) {

std::cout << "File was not opened\n";

return 1;

}

BBS BBS;

std::vector<bool> binary;

std::vector<uint8\_t> decimal;

std::bitset<8> b;

system("cls");

std::cout << "Сгенерированная LCG последовательность\n\nВ виде битовой строки:\n";

for (int i = 0; i < n + 1; i++) {

binary.push\_back(BBS.generate());

if (i != n)

std::cout << binary.back();

if (i % 8 == 0 && i != 0) {

decimal.push\_back(b.to\_ulong());

out.write(reinterpret\_cast<const char\*>(&decimal.back()), sizeof(uint8\_t));

}

b[i % 8] = binary.back();

}

std::cout << std::endl << "\nВ виде 8-битных чисел:\n";

for (int i = 0; i < decimal.size(); i++) {

std::cout << (int)decimal[i] << " ";

}

std::cout << std::endl << std::endl;

out.close();

system("pause");

return 0;

}

int LFSR\_init() {

system("cls");

uint n = 0, seed = 0, a = 0, c = 0, m = 0;

std::cout << "LFSR generator\n\nВведите требуемое количество 8-битных чисел\n>> ";

std::cin >> n;

std::ofstream out("generated\_LFSR.bin", std::ios::binary);

if (!out.is\_open()) {

std::cout << "File was not opened\n";

return 1;

}

LFSR LFSR;

std::vector<uint8\_t> decimal;

system("cls");

std::cout << "Сгенерированная LFSR последовательность\n\nВ виде битовой строки:\n";

for (int i = 0; i < n; i++) {

std::bitset<8> temp = LFSR.generate();

std::cout << temp;

decimal.push\_back(temp.to\_ulong());

out.write(reinterpret\_cast<const char\*>(&decimal.back()), sizeof(uint8\_t));

}

std::cout << std::endl << "\nВ виде 8-битных чисел:\n";

for (int i = 0; i < decimal.size(); i++) {

std::cout << (int)decimal[i] << " ";

}

std::cout << std::endl << std::endl;

out.close();

system("pause");

return 0;

}