

**МИНОБРНАУКИ РОССИИ**

**Федеральное государственное бюджетное образовательное учреждение  
высшего образования**

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

**Кафедра теоретических основ  
компьютерной безопасности и  
криптографии**

**Теория псевдослучайных генераторов**

**Практическая работа**

**ОТЧЕТ ПО ДИСЦИПЛИНЕ**

**«ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ»**

**студентки 4 курса 431 группы**

**специальности 10.05.01 «Компьютерная безопасность»**

**факультета компьютерных наук и информационных технологий**

**Кайдышевой Дарьи Сергеевны**

**Преподаватель**

**доцент, к. п. н.**

\_\_\_\_\_

**И. И. Слеповичев**

**Саратов 2024**

## СОДЕРЖАНИЕ

<b>1</b>	<b>Задание 1 Генератор псевдослучайных чисел .....</b>	<b>3</b>
1.1	Линейный конгруэнтный метод .....	4
1.2	Аддитивный метод.....	6
1.3	Пятипараметрический метод.....	7
1.4	Регистр сдвига с обратной связью (РСЛОС).....	9
1.5	Нелинейная комбинация РСЛОС .....	11
1.6	Вихрь Мерсенна .....	13
1.7	RC4.....	17
1.8	ГПСЧ на основе RSA .....	20
1.9	Алгоритм Блюма-Блюма-Шуба.....	22
<b>2</b>	<b>Задание 2 Преобразование ПСЧ к заданному распределению .....</b>	<b>24</b>
	<b>ПРИЛОЖЕНИЕ А.....</b>	<b>25</b>

## 1 Задание 1 Генератор псевдослучайных чисел

Создайте программу для генерации псевдослучайных величин следующими алгоритмами:

- a. Линейный конгруэнтный метод;
- b. Аддитивный метод;
- c. Пятипараметрический метод;
- d. Регистр сдвига с обратной связью (РСЛОС);
- e. Нелинейная комбинация РСЛОС;
- f. Вихрь Мерсенна;
- g. RC4;
- h. ГПСЧ на основе RSA;
- i. Алгоритм Блюма-Блюма-Шуба;

Название программы: prng.exe

Для управления приложением предлагается следующий формат параметров командной строки:

```
Командная строка
D:\tgpsch>prng.exe /h
Применение: prng.exe /g:<generator> [/n:<count>] [/f:<filename>] [/i:<params>]
prng.exe /h for help
Генерация последовательности псевдослучайных чисел по выбранному методу

Возможные аргументы:
/g: <generator> параметр указывает на метод генерации ПСЧ:
                  lc - линейный конгруэнтный метод;
                  add - аддитивный метод;
                  sp - пятипараметрический метод;
                  lfsr - регистр сдвига с обратной связью (РСЛОС);
                  nfsr - нелинейная комбинация РСЛОС;
                  mt - вихрь Мерсенна;
                  rc4 - RC4;
                  rsa - ГПСЧ на основе RSA;
                  bbs - алгоритм Блюма-Блюма-Шуба;
/n: <count>      количество генерируемых чисел (по умолчанию 10000)
/f: <filename>   полное имя файла, в который будут выводиться данные (по умолчанию rnd.dat)
/i: <params>     перечисление параметров для выбранного генератора
```

## Рисунок 1

Таблица 1. Порядок элементов вектора параметров (/i:)

Метод	Описание параметров
lc	Модуль, множитель, приращение, начальное значение
add	Модуль, младший индекс, старший индекс, последовательность начальных значений
5p	p, q1, q2, q3, w (см. лекции п. 3.5.2), начальное значение
lfsr	Двоичное представление вектора коэффициентов, начальное значение регистра
nfsr	В алгоритме использовать три РСЛОС R1, R2, R3, скомбинированных функцией $R1 \wedge R2 + R2 \wedge R3 + R3$ . Параметры – двоичное представление векторов коэффициентов для R1, R2, R3, w, x1, x2, x3. w – длина слова, x1, x2, x3 – десятичное представление начальных состояний регистров R1, R2, R3.
mt	Модуль, начальное значение x
rc4	256 начальных значений
rsa	Модуль n, число e, w, начальное значение x. e удовлетворяет условиям: $1 < e < (p-1)(q-1)$ , $\text{НОД}(e, (p-1)(q-1)) = 1$ , где $p \cdot q = n$ . x из интервала [1,n] w – длина слова.
bbs	Начальное значение x (взаимно простое с n). При генерации использовать параметры: $p = 127, q = 131, n = p \cdot q = 16637$

### 1.1 Линейный конгруэнтный метод

Последовательность ПСЧ, получается по формуле:

$$X_{n+1} = (aX_n + c) \bmod m, n \geq 1.$$

В его основе лежит выбор четырех ключевых параметров:

- $m > 0$ , модуль;
- $0 \leq a \leq m$ , множитель;
- $0 \leq c \leq m$ , приращение (инкремент);
- $0 \leq X_0 \leq m$ , начальное значение.

```
D:\tgpsch>prng.exe /g:lc /i:1024,171,513,577 /n:1200 /f:lc.dat
Числа сгенерированы и сохранены в файл lc.dat!

D:\tgpsch>_
```

## Рисунок 2 – Ввод



Рисунок 3 – Вывод

```

"""линейный конгруэнтный метод"""
def lc(m, a, c, x0, n_ = 10000):
    x = []
    x.append(x0);
    for i in range(1, n_ - 1):
        x.append(((a * x[i - 1] + c) % m) % 2**10)
    return x

```

Рисунок 4 – Алгоритм

## 1.2 Аддитивный метод

Последовательность ПСЧ, получается по формуле:

$$X_{n+1} = (X_{n-k} + X_{n-j}) \bmod m, \quad j > k \geq 1.$$

В его основе лежит выбор четырех ключевых параметров:

- $m > 0$ , модуль;
- $k$ , младший индекс;
- $j$ , старший индекс;
- последовательность из  $j$  начальных значений.

```
D:\tgpsch>prng.exe /g:add /i:1024,7,11,654,234,654,546,345,875,334,
345,765,546,998,34,756,987,544 /n:1200 /f:add.dat
Числа сгенерированы и сохранены в файл add.dat!

D:\tgpsch>
```

Рисунок 5 – Ввод

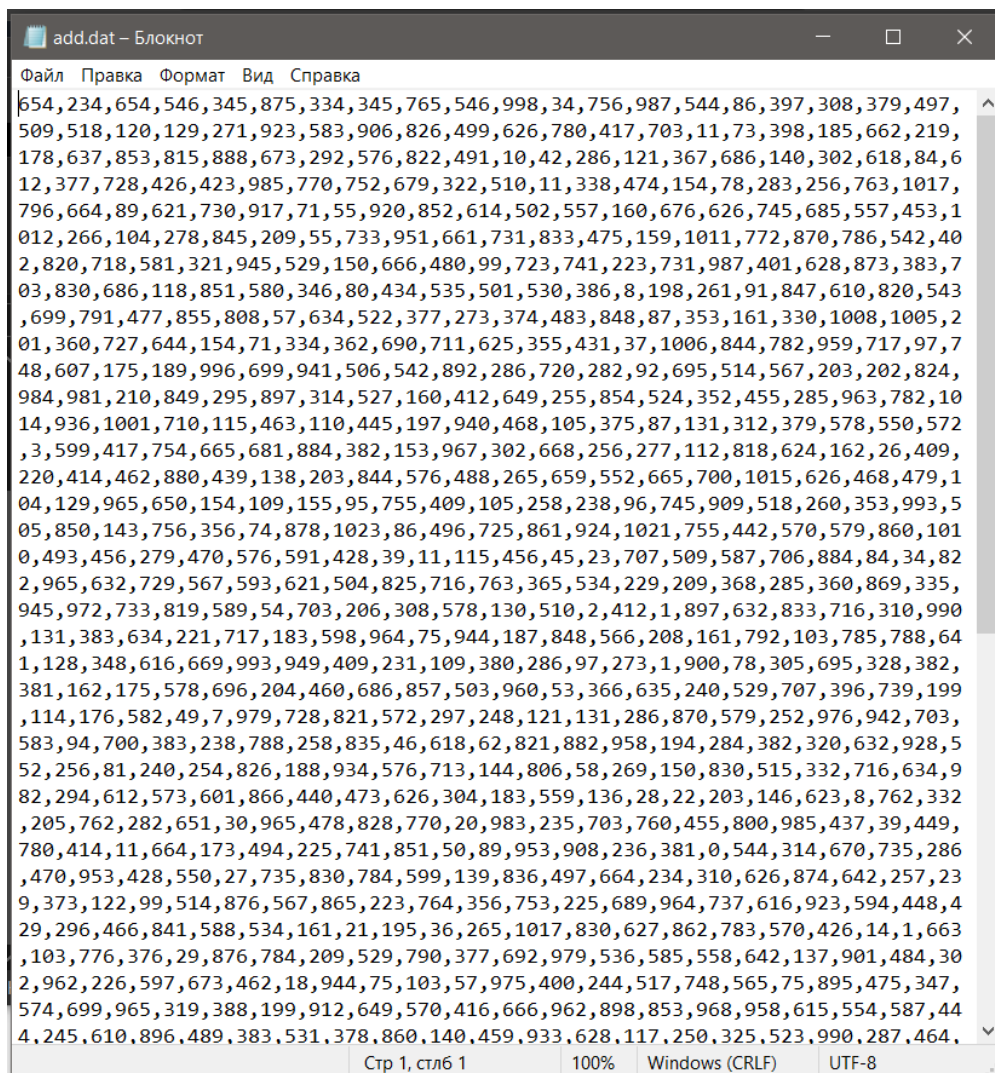


Рисунок 6 – Вывод

```
"""аддитивный метод"""
def add(m, low_i, up_i, start_seq, n_ = 10000):
    x = start_seq
    seq = start_seq.copy()
    n = len(seq)
    l = n_ - n
    for _ in range(1):
        xn = (seq[n - low_i] + seq[n - up_i]) % m
        x.append(xn % 2**10)
        seq.append(xn)
        del seq[0]
    return x
```

Рисунок 7 – Алгоритм

### 1.3 Пятипараметрический метод

Данный метод является частным случаем РСЛОС, использует характеристический многочлен из 5 членов и позволяет генерировать последовательности  $w$ -битовых двоичных целых чисел в соответствии со следующей рекуррентной формулой:

$$X_{n+p} = X_{n+q_1} + X_{n+q_2} + X_{n+q_3} + X_n, \quad n = 1, 2, 3, \dots$$

Параметры  $(p, q_1, q_2, q_3, w)$  и  $X_1, \dots, X_p$ , первоначально задают как начальный вектор.

```
D:\tgpsch>prng.exe /g:5p /i:107,31,57,82,10,11101010101101011010 /n
:1200 /f:5p.dat
Числа сгенерированы и сохранены в файл 5p.dat!
D:\tgpsch>
```

Рисунок 8 – Ввод





Рисунок 9 – Вывод

```

"""Sp"""
def _5p(p, q1, q2, q3, w, x0, n_ = 10000):
    x = []
    x0 = int(x0, 2)
    for _ in range(n_):
        cur = 0
        for _ in range(w):
            bit_q1 = (x0 >> p - q1) & 1
            bit_q2 = (x0 >> p - q2) & 1
            bit_q3 = (x0 >> p - q3) & 1
            bit_x0 = x0 & 1
            xor = bit_q1 ^ bit_q2 ^ bit_q3 ^ bit_x0
            cur = (cur << 1) | xor
            x0 = (x0 >> 1) | (xor << p - 1)
        x.append(cur % 2**10)
    return x

```

Рисунок 10 – Алгоритм



#### 1.4 Регистр сдвига с обратной связью (РСЛОС)

*Регистр сдвига с обратной линейной связью (РСЛОС)* – регистр сдвига битовых слов, у которого входной (вдвигаемый) бит является линейной функцией остальных битов. Вдвигаемый вычисленный бит заносится в ячейку с номером 0. Количество ячеек  $p$  называют длиной регистра.

Для натурального  $p$  и  $a_1, a_2, \dots, a_{p-1}$ , принимающих значения 0 или 1, определяют рекуррентную формулу:

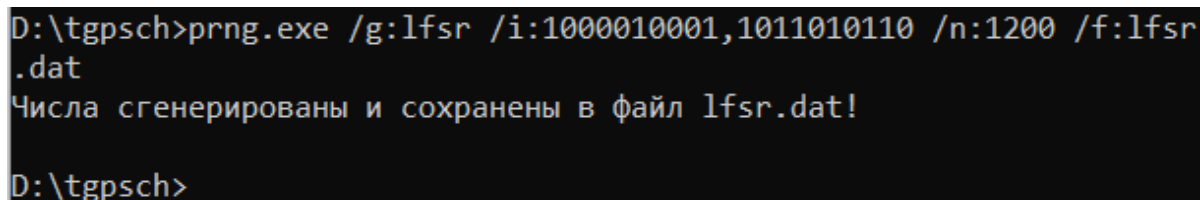
$$X_{n+p} = a_{p-1}X_{n+p-1} + a_{p-2}X_{n+p-2} + \dots + a_1X_{n+1} + X_n, \quad (1)$$

Как видно из формулы, для РСЛОС функция обратной связи является линейной булевой функцией от состояний всех или некоторых битов регистра.

Одна итерация алгоритма, генерирующего последовательность, состоит из следующих шагов:

1. Содержимое ячейки  $p - 1$  формирует очередной бит ПСП битов.
2. Содержимое ячейки 0 определяется значением функции обратной связи, являющейся линейной булевой функцией с коэффициентами  $a_1, a_2, \dots, a_{p-1}$ . Его вычисляют по формуле 1.
3. Содержимое каждого  $i$ -го бита перемещается в  $(i + 1)$ -й,  $0 \leq i < p - 1$ .
4. В ячейку 0 записывается новое содержимое, вычисленное на шаге 2.

Параметры: двоичное представление вектора коэффициентов, начальное значение регистра.



```
D:\tgpsch>prng.exe /g:lfsr /i:1000010001,1011010110 /n:1200 /f:lfsr .dat
Числа сгенерированы и сохранены в файл lfsr.dat!
D:\tgpsch>
```

Рисунок 11 – Ввод

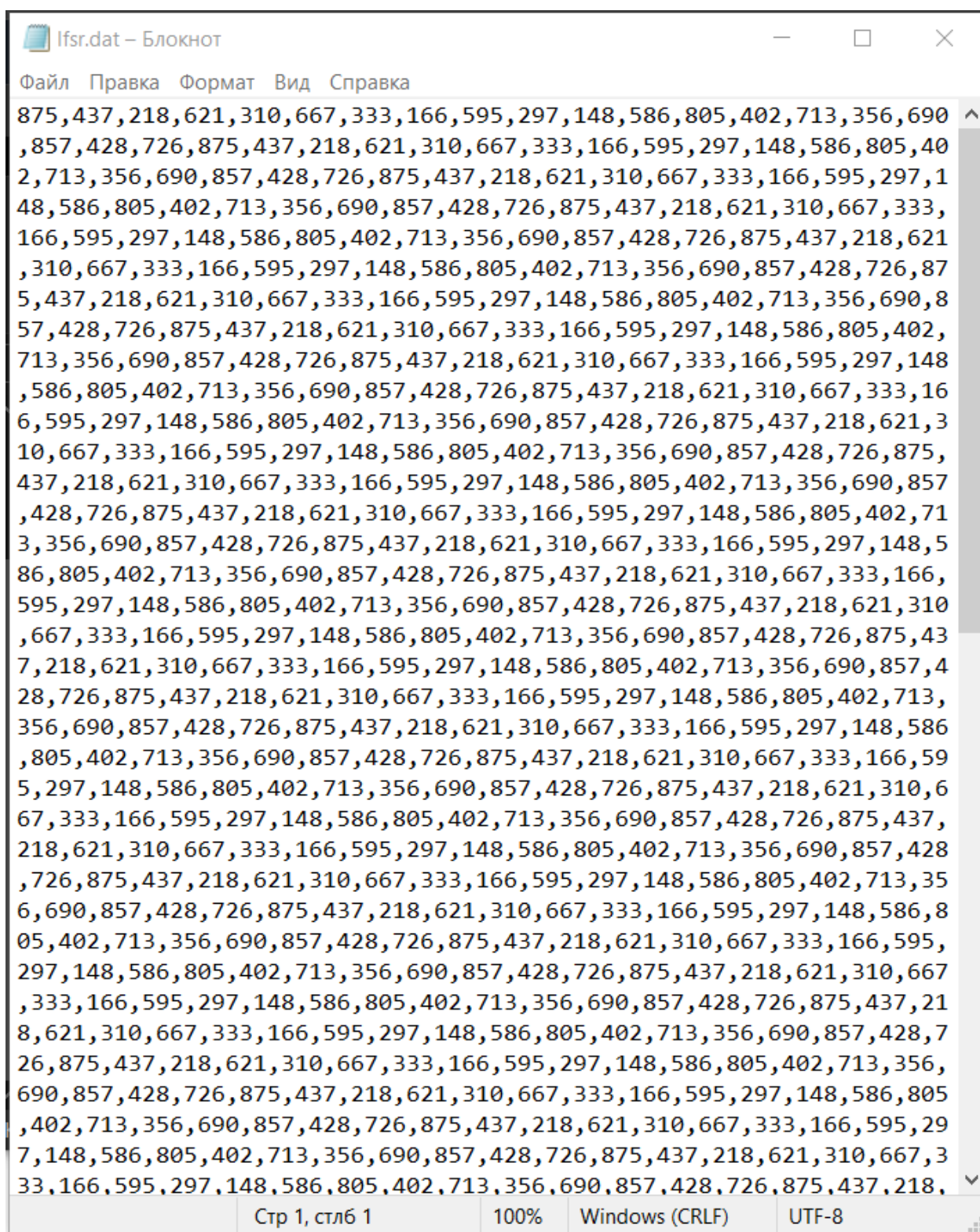


Рисунок 12 – Вывод

```

"""рслос"""
def lfsr(vec_bin, start_reg, n_ = 10000):
    x = []
    reg_len = len(start_reg)
    vec_bin = int(vec_bin, 2)
    start_reg = int(start_reg, 2)
    shift = reg_len - 1
    for _ in range(n_):
        new = (start_reg ^ vec_bin >> shift) & 1
        start_reg = (start_reg >> 1) | (new << (shift))
        x.append(start_reg % 2**10)
    return x

```

Рисунок 13 – Алгоритм

### 1.5 Нелинейная комбинация РСЛОС

Нелинейная функция генератора:

$$f(x_1, x_2, x_3) = x_1x_2 \oplus (1 + x_2)x_3 = x_1x_2 \oplus x_2x_3 \oplus x_3.$$

Параметры: двоичное представление вектора коэффициентов  $R_1, R_2, R_3$ .

```

D:\tgpsch>prng.exe /g:nfsr /i:1001110110,1011010110,1100101001,9,49
1,424,532 /n:1200 /f:nfsr.dat
Числа сгенерированы и сохранены в файл nfsr.dat!

D:\tgpsch>

```

Рисунок 14 – Ввод

nfsr.dat – Блокнот

Файл Правка Формат Вид Справка

309,275,241,80,463,325,195,65,63,21,12,507,342,306,238,90,54,18,14,5,508,340,204,68,60,20,12,4,3,510,341,307,238,421,355,222,437,364,292,227,417,159,117,44,484,163,414,373,300,283,265,248,424,152,119,466,334,197,444,363,294,285,267,249,87,50,494,165,412,372,211,433,144,399,378,297,280,264,248,87,461,187,105,39,29,11,6,509,340,307,273,240,431,357,220,436,147,398,378,214,77,452,323,318,277,268,260,252,84,51,494,346,201,440,360,216,72,56,23,498,337,304,272,240,80,48,16,15,506,342,205,443,150,397,379,214,434,145,399,133,124,468,179,401,143,122,470,178,110,37,483,161,96,479,330,313,279,242,430,154,118,45,484,348,203,441,151,114,465,335,197,67,62,490,166,98,33,480,351,309,236,420,156,116,44,27,502,338,206,69,451,190,405,371,209,79,58,489,344,311,274,270,250,86,50,17,496,336,207,442,361,295,226,417,352,288,224,95,458,326,194,65,448,320,192,64,63,490,345,311,237,91,54,493,347,201,71,61,20,499,337,207,69,60,491,345,200,440,151,397,132,387,382,298,230,93,459,185,104,472,183,402,369,303,229,92,459,326,317,276,268,251,425,152,392,135,386,382,213,435,145,112,464,176,111,474,329,312,279,269,251,86,461,324,316,235,422,354,222,74,57,488,344,200,71,450,321,319,234,422,157,395,134,386,129,384,383,298,281,264,263,258,257,256,256,255,426,358,221,436,364,219,438,365,292,284,244,83,462,325,316,276,243,430,357,291,225,95,53,19,14,506,169,408,375,301,228,419,353,223,74,454,189,404,371,302,282,246,82,49,495,165,99,33,31,10,505,343,205,68,451,321,192,447,362,294,226,94,53,492,347,310,274,241,431,154,393,376,296,231,418,353,288,287,266,262,253,427,153,119,45,27,9,7,2,510,170,102,34,30,10,6,2,1,511,170,409,375,210,433,367,218,438,146,113,464,335,314,278,242,81,463,186,406,141,388,380,212,76,59,489,167,98,478,181,403,142,389,380,299,281,247,82,462,186,105,472,328,199,445,148,396,132,124,43,486,349,308,275,270,261,259,254,426,153,392,376,215,434,366,218,73,455,189,107,38,482,161,415,138,390,130,126,42,25,503,173,100,476,180,108,36,28,11,505,168,408,136,120,40,24,8,7,509,171,102,477,331,198,445,363,217,72,455,322,318,234,89,456,327,317,235,89,55,18,497,336,304,239,421,156,395,377,215,77,59,22,498,174,101,476,331,313,232,423,354,289,287,245,83,49,16,496,175,410,374,210,78,58,22,13,507,169,103,34,481,351,202,441,360,295,285,244,428,155,393,135,125,43,25,8,504,168,103,477,180,403,369,208,432,144,112,47,485,163,97,32,480,160,96,32,31,501,172,411,374,301,283,246,429,356,291,286,266,249,424,359,290,286,245,428,356,220,75,454,322,193,447,149,115,46,485,348,308,236,91,457,184,407,370,302,229,419,158,394,134,125,468,332,196,67,449,191,106,473,328,312,232,88,55,493,164,412,139,390,381,299,230,418,158,117,467,177,111,37,28,500,172,100,35,481,160,415,373,211,78,453,323,193,64,448,191,405,140,388,131,385,128,384,128,127,469,179,110,474,182,109,475,182,402,142,122,41,487,162,414,138,121,471,178,401,368

Стр 1, стлб 1100%Windows (CRLF)UTF-8

Рисунок 15 – Вывод

```

"""нелинейная комбинация рслос"""
def nfsrc(R1, R2, R3, w, x1, x2, x3, n_ = 10000):
    x = []
    lR1 = len(R1)
    lR2 = len(R2)
    lR3 = len(R3)
    for _ in range(n_):
        cur = 0
        for _ in range(w):
            xorR1 = (x1 ^ (x1 >> lR1 - 1))
            xorR2 = (x2 ^ (x2 >> lR2 - 1))
            xorR3 = (x3 ^ (x3 >> lR3 - 1))
            res = ((xorR1 ^ xorR2) + (xorR2 ^ xorR3) + xorR3) & 1
            x1 = (x1 >> 1) | (res << lR1 - 1)
            x2 = (x2 >> 1) | (res << lR2 - 1)
            x3 = (x3 >> 1) | (res << lR3 - 1)
            cur = (cur << 1) | res
        x.append(cur % 2**10)
    return x

```

Рисунок 16 – Алгоритм

## 1.6 Вихрь Мерсенна

Метод Вихрь Мерсенна позволяет генерировать последовательность двоичных псевдослучайных целых  $w$ -битовых чисел в соответствии со следующей рекуррентной формулой

$$X_{n+p} = X_{n+q} \oplus (X_n^r | X_{n+1}^l)A \quad (n = 0, 1, 2, \dots),$$

где  $p, q, r$  – целые константы,  $p$  – степень рекуррентности,  $1 \leq q \leq p$ ;

$X_n$  –  $w$ -битовое двоичное целое число;

$(X_n^r | X_{n+1}^l)$  – двоичное целое число, полученное конкатенацией чисел  $X_n^r$  и  $X_{n+1}^l$ , когда первые  $(w-r)$  битов взяты из  $X_n$ , а последние  $r$  битов из  $X_{n+1}$  в том же порядке;

$A$  – матрица размера  $w \times w$ , состоящая из нулей и единиц, определенная посредством  $a$ ;

$XA$  – произведение, при вычислении которого сначала выполняют операцию  $X \gg 1$  (сдвига битов на одну позицию вправо), если последний бит  $X$  равен 0, а затем, когда последний бит  $X = 1$ , вычисляют  $XA = (X \gg 1) \oplus a$ ,

$$a = (a_{w-1}, a_{w-2}, \dots, a_0),$$

$$X = (x_{w-1}, x_{w-2}, \dots, x_0),$$

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & 1 & & & 0 \\ 0 & 0 & 0 & \ddots & & 0 \\ \vdots & \dots & \dots & & \ddots & \vdots \\ 0 & 0 & & & & 1 \\ a_{w-1} & a_{w-2} & \dots & \dots & \dots & a_0 \end{pmatrix}.$$

Алгоритм Вихрь Мерсенна состоит из попеременного выполнения процедур *рекурсивной генерации* и «заковки». Рекурсивная генерация представляет из себя РСЛОС с дополнительной рекурсивной функцией для потока выходных битов. Операция «заковки» является процедурой, усиливающей равномерность распределения на больших размерностях битовых векторов.

### Шаги алгоритма.

**Шаг 1а.** Инициализируются значения  $u, h, a$  по формуле:

$u := (1, 0, \dots, 0)$  – всего  $w - r$  бит,  $h := (0, 1, \dots, 1)$  – всего  $r$  бит,

$a := (a_{w-1}, a_{w-2}, \dots, a_0)$  – последняя строка матрицы  $A$ .

**Шаг 1б.**  $X_0, X_1, \dots, X_{p-1}$  заполняются начальными значениями.

**Шаг 2.** Вычисляется  $Y := (y_0, y_1, \dots, y_{w-1}) := (X_n^r | X_{n+1}^l)$ .

**Шаг 3.** Вычисляется новое значение  $X_i$ :

$X_n := X_{(n+q) \bmod p} \oplus (Y \gg 1) \oplus a$ , если младший бит  $y_0 = 1$ ;

$X_n := X_{(n+q) \bmod p} \oplus (Y \gg 1) \oplus 0$ , если младший бит  $y_0 = 0$ ;

**Шаг 4.** Вычисляется  $X_i T$ .

$$Y := X_n,$$



$$Y := Y \oplus (Y \gg u),$$

$$Y := Y \oplus ((Y \ll s) \cdot b),$$

$$Y := Y \oplus ((Y \ll t) \cdot c),$$

$$Z := Y \oplus (Y \gg l).$$

Z подается на выход, как результат.

**Шаг 5.**  $n := (n + 1) \bmod p$ . Переход на шаг 2.

```
D:\tgpsch>prng.exe /g:mt /i:4563 /n:1200 /f:mt.dat
Числа сгенерированы и сохранены в файл mt.dat!

D:\tgpsch>
```

Рисунок 17 – Ввод

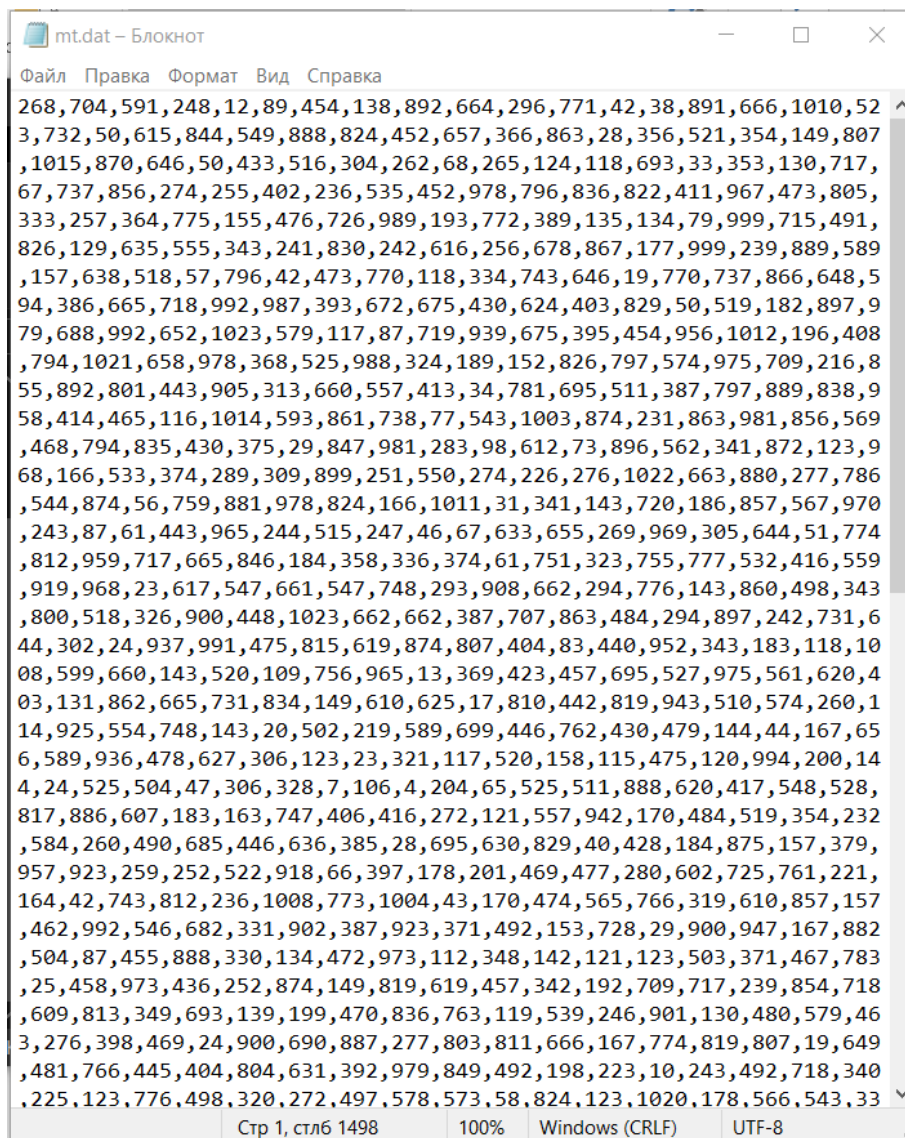


Рисунок 18 – Вывод



```

"""вихрь мерсенна"""
def mt(x0, n = 624, n_ = 10000):
    w = 32
    r = 31
    m = 397
    a = 0x9908B0DF
    u = 11
    d = 0xFFFFFFFF
    s = 7
    t = 15
    l = 18
    b = 0x9D2C5680
    c = 0xEFC60000
    f = 1812433253
    lst = [0] * n
    ind = n + 1

    def f1(core):
        lst[0] = core
        for i in range(1, n):
            tmp = f * (lst[i - 1] ^ (lst[i - 1] >> (w - 2))) + i
            lst[i] = tmp & d

    def f2():
        nonlocal ind
        if ind >= n:
            f3()
            ind = 0

```

Рисунок 19 – Алгоритм 1

```

→ ind = 0
→ y = lst[ind]
→ y = y ^ ((y >> u) & d)
→ y = y ^ ((y << s) & b)
→ y = y ^ ((y << t) & c)
→ y = y ^ (y >> 1)
→ ind = ind + 1
→ return y & d

def f3():
    for i in range(n):
        x = (lst[i] >> r) + (lst[(i + 1) % n] & ((1 << r) - 1))
        x_a = x >> 1
        lst[i] = lst[(i + m) % n] ^ x_a
        if (x % 2) != 0:
            lst[i] ^= a

    f1(x0)
    res = []
    for _ in range(n_):
        o = f2()
        res.append(o % 2**10)
    return res

```

Рисунок 20 – Алгоритм 2

**Параметры алгоритма Вихрь Мерсенна:**  $p = 624$ ,  $w = 32$ ,  $r = 31$ ,  $q = 397$ ,  $a = 2567483615$  ( $9908B0DF_{16}$ ),  $u = 11$ ,  $s=7$ ,  $t=15$ ,  $l = 18$ ,  $b = 2636928640$  ( $9D2C5680_{16}$ ),  $c = 4022730752$  ( $EFC60000_{16}$ ).

Вводимые параметры: начальное значение.

## 1.7 RC4

### Описание алгоритма.

1. Инициализация  $S_i$ ,  $i = 0, 1, \dots, 255$ .

a) *for*  $i = 0$  to 255:  $S_i = i$ ;

b)  $j = 0$ ;

c) *for*  $i = 0$  to 255:  $j = (j + S_i + K_i) \bmod 256$ ;  $Swap(S_i, S_j)$

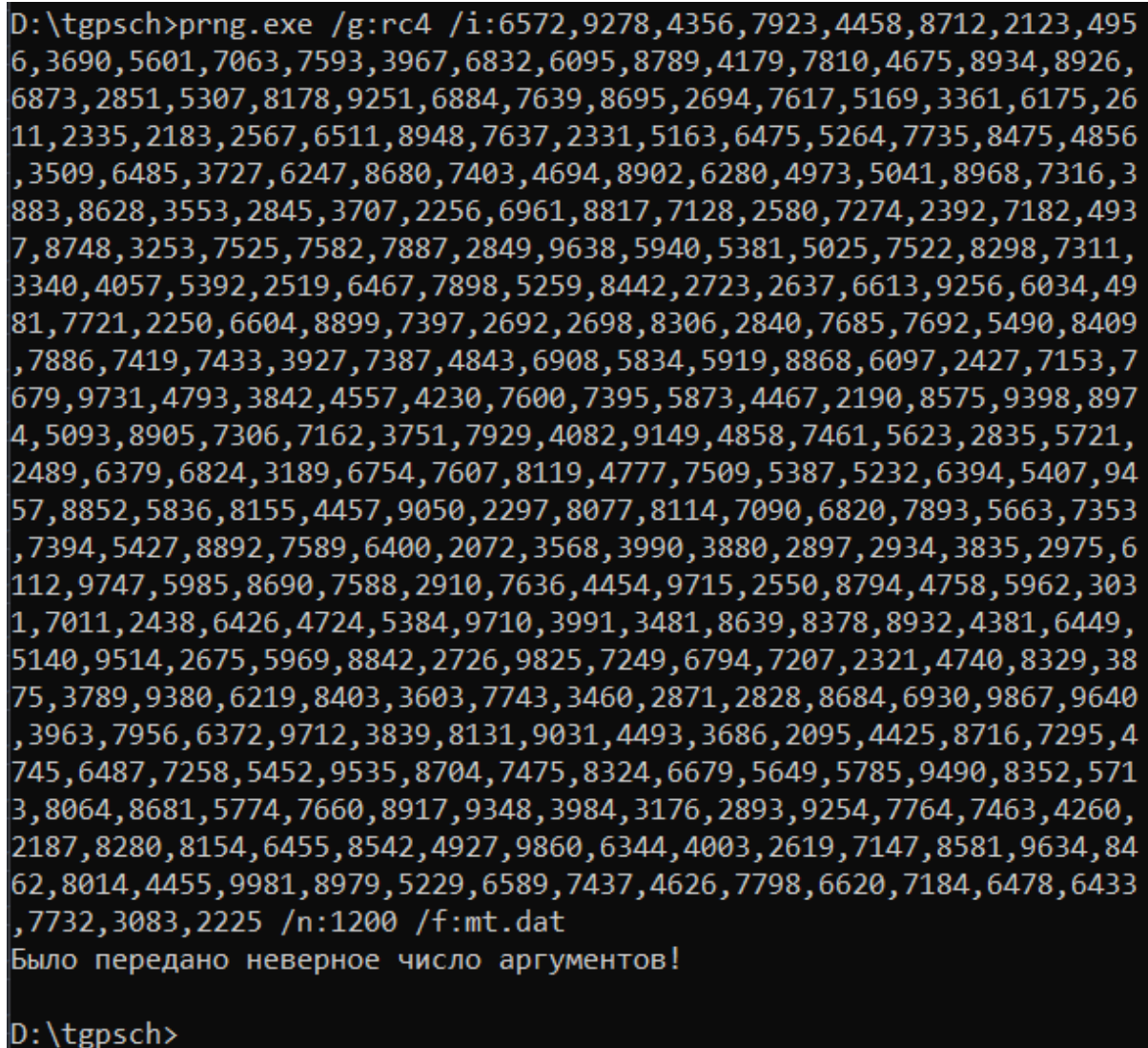
2.  $i = 0, j = 0$ .

3. Итерация алгоритма:

a)  $i = (i + 1) \bmod 256$ ;

- b)  $j = (j + S_i) \bmod 256$ ;
- c)  $Swap(S_i, S_j)$ ;
- d)  $t = (S_i + S_j) \bmod 256$ ;
- e)  $K = S_t$ ;

Параметры: 256 начальных значений.



```
D:\tgpsch>prng.exe /g:rc4 /i:6572,9278,4356,7923,4458,8712,2123,495
6,3690,5601,7063,7593,3967,6832,6095,8789,4179,7810,4675,8934,8926,
6873,2851,5307,8178,9251,6884,7639,8695,2694,7617,5169,3361,6175,26
11,2335,2183,2567,6511,8948,7637,2331,5163,6475,5264,7735,8475,4856
,3509,6485,3727,6247,8680,7403,4694,8902,6280,4973,5041,8968,7316,3
883,8628,3553,2845,3707,2256,6961,8817,7128,2580,7274,2392,7182,493
7,8748,3253,7525,7582,7887,2849,9638,5940,5381,5025,7522,8298,7311,
3340,4057,5392,2519,6467,7898,5259,8442,2723,2637,6613,9256,6034,49
81,7721,2250,6604,8899,7397,2692,2698,8306,2840,7685,7692,5490,8409
,7886,7419,7433,3927,7387,4843,6908,5834,5919,8868,6097,2427,7153,7
679,9731,4793,3842,4557,4230,7600,7395,5873,4467,2190,8575,9398,897
4,5093,8905,7306,7162,3751,7929,4082,9149,4858,7461,5623,2835,5721,
2489,6379,6824,3189,6754,7607,8119,4777,7509,5387,5232,6394,5407,94
57,8852,5836,8155,4457,9050,2297,8077,8114,7090,6820,7893,5663,7353
,7394,5427,8892,7589,6400,2072,3568,3990,3880,2897,2934,3835,2975,6
112,9747,5985,8690,7588,2910,7636,4454,9715,2550,8794,4758,5962,303
1,7011,2438,6426,4724,5384,9710,3991,3481,8639,8378,8932,4381,6449,
5140,9514,2675,5969,8842,2726,9825,7249,6794,7207,2321,4740,8329,38
75,3789,9380,6219,8403,3603,7743,3460,2871,2828,8684,6930,9867,9640
,3963,7956,6372,9712,3839,8131,9031,4493,3686,2095,4425,8716,7295,4
745,6487,7258,5452,9535,8704,7475,8324,6679,5649,5785,9490,8352,571
3,8064,8681,5774,7660,8917,9348,3984,3176,2893,9254,7764,7463,4260,
2187,8280,8154,6455,8542,4927,9860,6344,4003,2619,7147,8581,9634,84
62,8014,4455,9981,8979,5229,6589,7437,4626,7798,6620,7184,6478,6433
,7732,3083,2225 /n:1200 /f:mt.dat
Было передано неверное число аргументов!

D:\tgpsch>
```

Рисунок 21 – Ввод

rc4.dat – Блокнот

Файл Правка Формат Вид Справка

```
6,85,60,3,91,253,243,54,58,179,63,32,44,86,60,60,205,235,7,27,148,1
0,64,190,205,29,198,243,162,234,68,135,108,245,72,243,49,251,107,12
,204,140,234,105,86,145,115,93,128,56,144,146,60,53,35,182,181,3,35
,134,192,103,247,49,126,75,129,155,107,221,233,190,12,233,132,220,3
6,53,84,85,49,202,67,4,57,163,213,123,51,230,231,148,181,97,35,161,
74,36,62,173,206,22,10,142,25,8,219,172,155,192,204,223,66,20,108,1
48,41,39,138,242,237,18,162,162,203,163,237,171,250,211,101,25,139,
7,179,13,145,146,62,56,216,222,20,134,245,111,81,168,104,205,202,25
3,35,95,229,30,48,157,196,26,208,162,5,163,132,101,234,220,127,176,
9,1,152,119,75,104,186,159,208,167,150,205,105,27,24,195,132,55,146
,21,49,177,11,34,167,201,24,198,150,101,179,39,246,11,229,129,30,15
0,217,44,1,124,175,221,25,117,117,38,16,52,65,141,41,141,80,182,190
,123,254,104,99,198,160,52,240,219,129,36,150,253,71,182,153,70,227
,90,78,33,215,202,41,36,253,61,89,108,26,17,35,16,186,60,11,108,90,
51,199,201,241,143,142,163,147,167,6,234,19,154,60,211,32,92,136,24
4,106,160,94,129,218,212,56,159,228,86,245,168,130,142,229,108,71,1
18,52,113,152,1,159,20,98,11,163,127,115,228,167,129,58,106,114,249
,61,234,17,163,226,210,253,165,119,197,117,141,101,72,48,201,51,70,
172,248,92,249,221,26,11,242,170,172,69,111,123,224,150,215,108,81,
164,208,179,238,66,190,103,247,140,69,207,47,255,9,90,77,125,69,192
,220,35,107,71,204,75,179,243,250,101,18,230,125,211,3,8,89,229,200
,98,38,26,135,198,22,249,0,205,200,121,115,17,31,7,229,62,11,145,13
0,83,253,9,241,199,168,172,37,32,4,220,251,253,194,224,109,220,78,5
0,42,62,76,223,89,159,32,71,176,88,212,211,104,238,169,113,171,74,4
9,238,164,250,206,94,24,1,205,67,235,199,9,105,191,239,152,82,71,11
7,112,50,198,194,64,11,45,44,175,53,164,116,252,11,134,228,5,227,26
,225,91,54,90,255,30,38,116,196,68,145,77,25,78,222,123,52,154,120,
53,89,29,34,189,109,79,202,231,210,32,63,148,119,104,244,29,250,203
,201,25,119,105,131,52,183,103,203,48,38,194,250,105,242,162,8,57,7
2,179,124,12,86,73,192,87,98,193,61,20,239,246,99,118,255,156,225,4
8,253,224,132,207,102,239,133,222,118,102,188,110,158,120,249,143,6
2,121,130,129,225,222,160,233,93,148,43,165,172,104,142,28,195,88,6
2,166,166,139,53,122,56,122,10,227,144,189,251,25,163,29,165,87,152
,254,95,55,91,1,51,14,167,230,90,27,161,137,144,183,63,90,204,229,1
85,190,105,244,223,97,247,50,205,132,133,66,165,21,73,34,229,88,247
,73,222,123,197,39,192,225,245,152,41,237,2,29,56,145,169,205,102,7
```

Стр 1, столб 1      100%      Windows (CRLF)      UTF-8

Рисунок 22 – Вывод

```

"""rc4"""
def rc4(k, count_num = 10000):
    len_k = len(k)
    S = [i for i in range(256)]
    j = 0
    for i in range(256):
        j = (j + S[i] + k[i % len_k]) % 256
        S[i], S[j] = S[j], S[i]
    i = 0
    j = 0
    Ks = []
    for _ in range(1, count_num + 1):
        i = (i + 1) % 256
        j = (j + S[i]) % 256
        S[i], S[j] = S[j], S[i]
        cur = S[(S[i] + S[j]) % 256]
        Ks.append(cur % 2**10)
    return Ks

```

Рисунок 23 – Алгоритм

## 1.8 ГПСЧ на основе RSA

### Описание алгоритма:

1. Сгенерировать два секретных простых числа  $p$  и  $q$ , а также  $n = pq$  и  $f = (p - 1)(q - 1)$ . Выбрать случайное целое число  $e$ ,  $1 < e < f$ , такое что  $\text{НОД}(e, f) = 1$ .
2. Выбрать случайное целое  $x_0$  – начальный вектор из интервала  $[1, n - 1]$ .
3. *For*  $i = 1$  *to*  $l$  *do*
  - a.  $x_i \leftarrow x_{i-1}^e \bmod n$ .
  - b.  $z_i \leftarrow$  последний значащий бит  $x_i$
4. Вернуть  $z_1, z_2, \dots, z_l$ .



Параметры: Модуль  $n$ , число  $e$ ,  $w$ , начальное значение  $x$ .  $e$  удовлетворяет условиям:  $1 < e < (p-1)(q-1)$ ,  $\text{НОД}(e, (p-1)(q-1)) = 1$ , где  $p * q = n$ ,  $x \in [1, n]$ ,  $w$  – длина слова.

```
D:\tgpsch>prng.exe /g:rsa /i:10967,571,77,10 /n:1200 /f:rsa.dat
Числа сгенерированы и сохранены в файл rsa.dat!

D:\tgpsch>
```

Рисунок 24 – Ввод

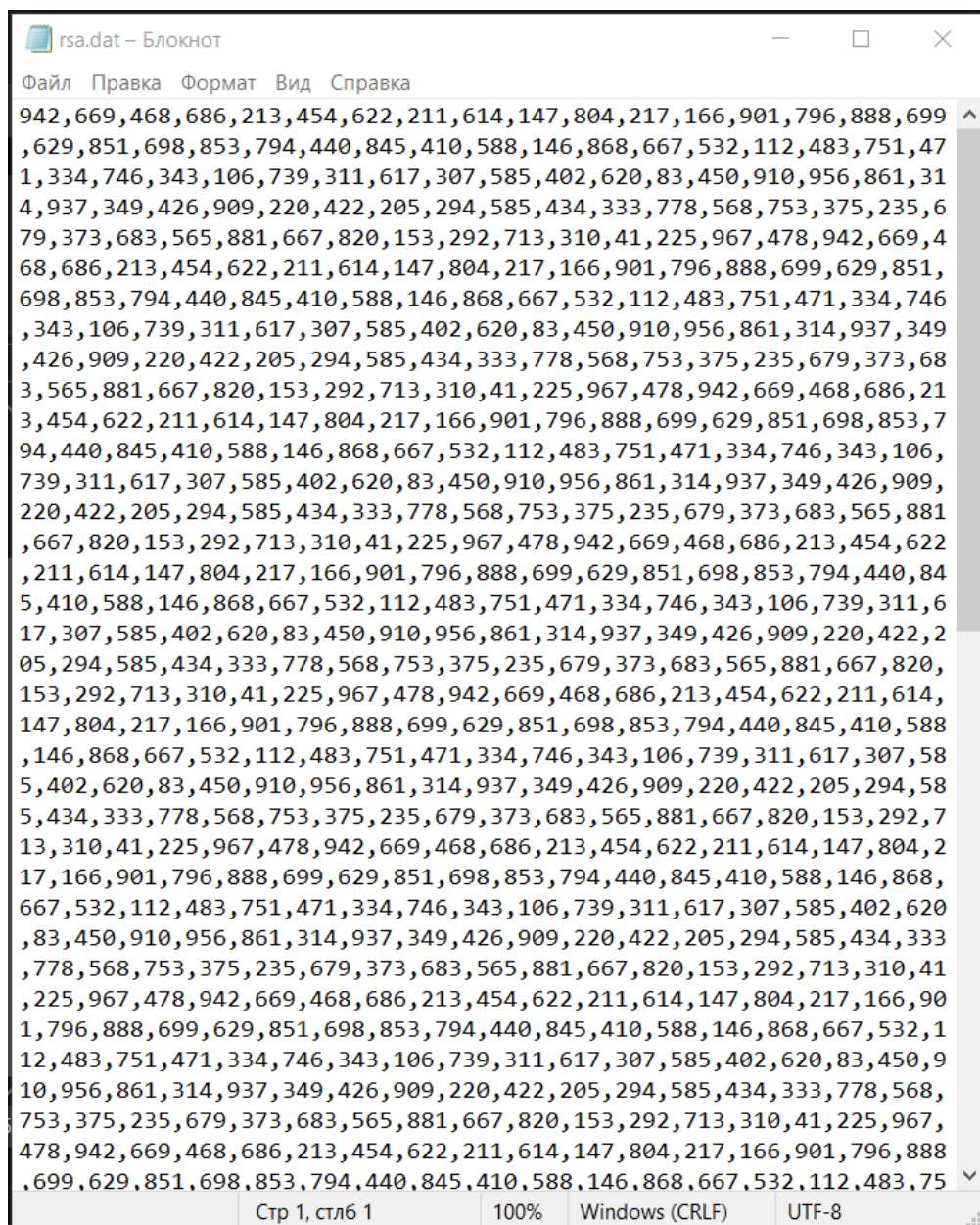


Рисунок 25 – Вывод

```

"""ГПСЧ на основе rsa"""
def rsa(n, e, w, x0, n_ = 10000):
    x = []
    for _ in range(n_):
        cur = 0
        for _ in range(w):
            x0 = pow(x0, e, n)
            cur = (cur << 1) | (x0 & 1)
        x.append(cur % 2**10)
    return x

```

Рисунок 26 – Алгоритм

### 1.9 Алгоритм Блюма-Блюма-Шуба

#### Описание алгоритма:

**На входе:** Длина  $l$ .

**На выходе:** Последовательность псевдослучайных бит  $z_1, z_2, \dots, z_l$ .

1. Сгенерировать два простых числа  $p$  и  $q$ , сравнимых с 3 по модулю 4. Это гарантирует, что каждый квадратичный вычет имеет один квадратный корень, который также является квадратичным вычетом. Произведение этих чисел –  $n=pq$  является целым числом Блюма. Выберем другое случайное целое число  $x$ , взаимно простое с  $n$ .
2. Вычислим  $x_0 = x^2 \bmod n$ , которое будет начальным вектором.
3. *For*  $i = 1$  *to*  $l$  *do*
  1.  $x_i \leftarrow x_{i-1}^2 \bmod n$ .
  2.  $z_i \leftarrow$  последний значащий бит  $x_i$
4. Вернуть  $z_1, z_2, \dots, z_l$ .

Интересным достоинством этого генератора является то, что для получения  $i$ -го бита  $b_i$  при известных  $p$  и  $q$  достаточно воспользоваться формулой



$$b_i = x_0^{2^i \bmod ((p-1)(q-1))} \bmod 2.$$

Параметры: начальное значение и длина слова.

```
D:\tgpsch>prng.exe /g:bbs /i:791,5 /n:1200 /f:bbs.dat
Числа сгенерированы и сохранены в файл bbs.dat!

D:\tgpsch>
```

Рисунок 27 – Ввод

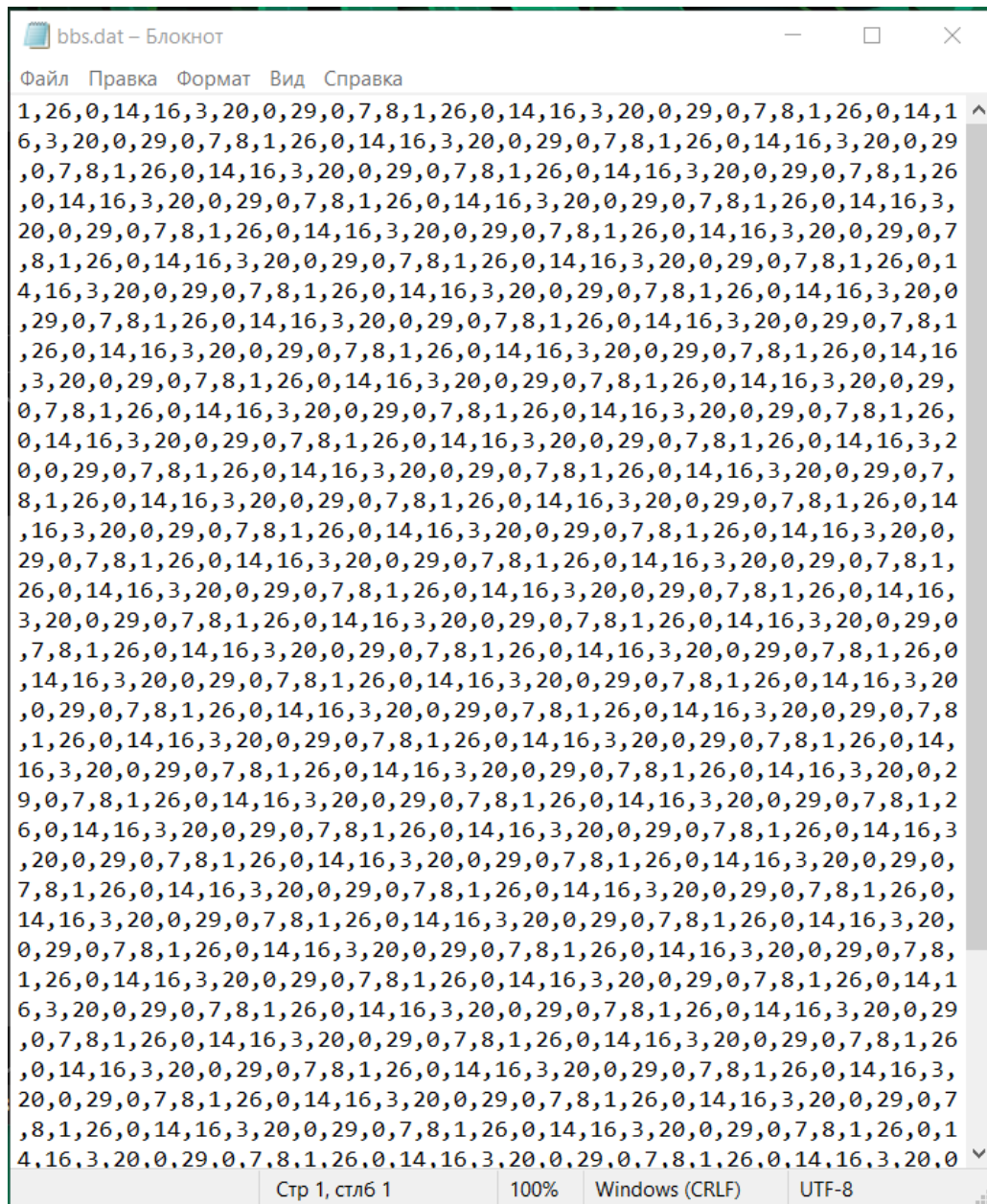


Рисунок 28 – Вывод

```

"""алгоритм блюма-блюма-шуба"""
def bbs(x0, l, n_ = 10000):
    p = 127
    q = 131
    n = p * q
    x = []
    for _ in range(n_):
        cur = 0
        for _ in range(l):
            x0 = pow(x0, 2, n)
            cur = (cur << 1) | (x0 & 1)
        x.append(cur % 2**10)
    return x

```

Рисунок 29 – Алгоритм

## 2 Задание 2 Преобразование ПСЧ к заданному распределению

## ПРИЛОЖЕНИЕ А

### Листинг Задание 1 Генератор псевдослучайных чисел

```
import sys
"""линейный конгруэнтный метод"""
def lc (m, a, c, x0, n_ = 10000):
    x = []
    x.append(x0);
    for i in range(1, n_ - 1):
        x.append(((a * x[i - 1] + c) % m) % 2**10)
    return x

"""аддитивный метод"""
def add(m, low_i, up_i, start_seq, n_ = 10000):
    x = start_seq
    seq = start_seq.copy()
    n = len(seq)
    l = n_ - n
    for _ in range(l):
        xn = (seq[n - low_i] + seq[n - up_i]) % m
        x.append(xn % 2**10)
        seq.append(xn)
        del seq[0]
    return x

"""5p"""
def _5p(p, q1, q2, q3, w, x0, n_ = 10000):
    x = []
    x0 = int(x0, 2)
    for _ in range(n_):
        cur = 0
        for _ in range(w):
            bit_q1 = (x0 >> p - q1) & 1
            bit_q2 = (x0 >> p - q2) & 1
            bit_q3 = (x0 >> p - q3) & 1
            bit_x0 = x0 & 1
            xor = bit_q1 ^ bit_q2 ^ bit_q3 ^ bit_x0
            cur = (cur << 1) | xor
            x0 = (x0 >> 1) | (xor << p - 1)
        x.append(cur % 2**10)
    return x

"""рслос"""
def lfsr(vec_bin, start_reg, n_ = 10000):
    x = []
    reg_len = len(start_reg)
    vec_bin = int(vec_bin, 2)
    start_reg = int(start_reg, 2)
    shift = reg_len - 1
    for _ in range(n_):
        new = (start_reg ^ vec_bin >> shift) & 1
        start_reg = (start_reg >> 1) | (new << (shift))
        x.append(start_reg % 2**10)
    return x

"""нелинейная комбинация рслос"""
def nlsr(R1, R2, R3, w, x1, x2, x3, n_ = 10000):
    x = []
    lR1 = len(R1)
    lR2 = len(R2)
    lR3 = len(R3)
    for _ in range(n_):
```

```

cur = 0
for _ in range(w):
    xorR1 = (x1 ^ (x1 >> lR1 - 1))
    xorR2 = (x2 ^ (x2 >> lR1 - 1))
    xorR3 = (x3 ^ (x3 >> lR1 - 1))
    res = ((xorR1 ^ xorR2) + (xorR2 ^ xorR3) + xorR3) & 1
    x1 = (x1 >> 1) | (res << lR1 - 1)
    x2 = (x2 >> 1) | (res << lR2 - 1)
    x3 = (x3 >> 1) | (res << lR3 - 1)
    cur = (cur << 1) | res
x.append(cur % 2**10)
return x

"""вихрь мерсенна"""
def mt(x0, n = 624, n_ = 10000):
    w = 32
    r = 31
    m = 397
    a = 0x9908B0DF
    u = 11
    d = 0xFFFFFFFF
    s = 7
    t = 15
    l = 18
    b = 0x9D2C5680
    c = 0xEFC60000
    f = 1812433253
    lst = [0] * n
    ind = n + 1

    def f1(core):
        lst[0] = core
        for i in range(1, n):
            tmp = f * (lst[i - 1] ^ (lst[i - 1] >> (w - 2))) + i
            lst[i] = tmp & d

    def f2():
        nonlocal ind
        if ind >= n:
            f3()
            ind = 0
        y = lst[ind]
        y = y ^ ((y >> u) & d)
        y = y ^ ((y << s) & b)
        y = y ^ ((y << t) & c)
        y = y ^ (y >> l)
        ind = ind + 1
        return y & d

    def f3():
        for i in range(n):
            x = (lst[i] >> r) + (lst[(i + 1) % n] & ((1 << r) - 1))
            x_a = x >> 1
            lst[i] = lst[(i + m) % n] ^ x_a
            if (x % 2) != 0:
                lst[i] ^= a

    f1(x0)
    res = []
    for _ in range(n_):
        o = f2()
        res.append(o % 2**10)
    return res

```

```

"""rc4"""
def rc4(k, count_num = 10000):
    len_k = len(k)
    S = [i for i in range(256)]
    j = 0
    for i in range(256):
        j = (j + S[i] + k[i % len_k]) % 256
        S[i], S[j] = S[j], S[i]
    i = 0
    j = 0
    Ks = []
    for _ in range(1, count_num + 1):
        i = (i + 1) % 256
        j = (j + S[i]) % 256
        S[i], S[j] = S[j], S[i]
        cur = S[(S[i] + S[j]) % 256]
        Ks.append(cur % 2**10)
    return Ks

"""ПСЧ на основе rsa"""
def rsa(n, e, w, x0, n_ = 10000):
    x = []
    for _ in range(n_):
        cur = 0
        for _ in range(w):
            x0 = pow(x0, e, n)
            cur = (cur << 1) | (x0 & 1)
        x.append(cur % 2**10)
    return x

"""алгоритм блюма-блума-шуба"""
def bbs(x0, l, n_ = 10000):
    p = 127
    q = 131
    n = p * q
    x = []
    for _ in range(n_):
        cur = 0
        for _ in range(l):
            x0 = pow(x0, 2, n)
            cur = (cur << 1) | (x0 & 1)
        x.append(cur % 2**10)
    return x

def generate_pseudo_random(method, args, n):
    if method == 'lc':
        int_values = [int(x) for x in args.split(',')]
        if len(int_values) != 4:
            print('Было передано неверное число аргументов!')
            return []
        m, a, c, x0 = int_values
        return lc(m, a, c, x0, n)

    elif method == 'add':
        args_split = args.split(',')
        if len(args_split) < 4:
            print('Было передано неверное число аргументов!')
            return []
        m = int(args_split[0])
        low_i = int(args_split[1])
        up_i = int(args_split[2])
        start_seq = list(map(int, args_split[3:]))

```

```

        return add(m, low_i, up_i, start_seq, n)

elif method == '5p':
    args_split = args.split(',')
    if len(args_split) != 6:
        print('Было передано неверное число аргументов!')
        return []
    p = int(args_split[0])
    q1 = int(args_split[1])
    q2 = int(args_split[2])
    q3 = int(args_split[3])
    w = int(args_split[4])
    x0 = args_split[5]
    return _5p(p, q1, q2, q3, w, x0, n)

elif method == 'lfsr':
    args_split = args.split(',')
    if len(args_split) != 2:
        print('Было передано неверное число аргументов!')
        return []
    vec_bin = args_split[0]
    start_reg = args_split[1]
    return lfsr(vec_bin, start_reg, n)

elif method == 'nfsr':
    args_split = args.split(',')
    if len(args_split) != 7:
        print('Было передано неверное число аргументов!')
        return []
    R1 = args_split[0]
    R2 = args_split[1]
    R3 = args_split[2]
    w = int(args_split[3])
    x1 = int(args_split[4])
    x2 = int(args_split[5])
    x3 = int(args_split[6])
    return nfsr(R1, R2, R3, w, x1, x2, x3, n)

elif method == 'mt':
    args_split = args.split(',')
    if len(args_split) != 1:
        print('Было передано неверное число аргументов!')
        return []
    x0 = int(args_split[0])
    return mt(x0, 624, n)

elif method == 'rc4':
    args_split = args.split(',')
    if len(args_split) != 256:
        print('Было передано неверное число аргументов!')
        return []
    k = list(map(int, args_split))
    return rc4(k, n)

elif method == 'rsa':
    args_split = args.split(',')
    if len(args_split) != 4:
        print('Было передано неверное число аргументов!')
        return []
    m, e, w, x0 = map(int, args_split)
    return rsa(m, e, w, x0, n)

elif method == 'bbs':

```

```

args_split = args.split(',')
if len(args_split) != 2:
    print('Было передано неверное число аргументов!')
    return []
x0 = int(args_split[0])
l = int(args_split[1])
return bbs(x0, l, n)

else:
    print("Введенный метод не предусмотрен или не существует!")
    return []

def print_usage():
    print('Применение: prng.exe /g:<generator> [/n:<count>] [/f:<filename>] [/i:<params>]')
    print('          prng.exe /h for help')

def print_help():
    print_usage()
    print('Генерация последовательности псевдослучайных чисел по выбранному методу')
    print()
    print('Возможные аргументы:')
    print('  /g: <generator>  параметр указывает на метод генерации ПСЧ:')
    print('                    lc  - линейный конгруэнтный метод;')
    print('                    add - аддитивный метод;')
    print('                    5p  - пятипараметрический метод;')
    print('                    lfsr - регистр сдвига с обратной связью (РСЛОС);')
    print('                    nfsr - нелинейная комбинация РСЛОС;')
    print('                    mt  - вихрь Мерсенна;')
    print('                    rc4 - RC4;')
    print('                    rsa - ГПСЧ на основе RSA;')
    print('                    bbs - алгоритм Блюма-Блюма-Шуба;')
    print('  /n: <count>      количество генерируемых чисел (по умолчанию 10000)')
    print('  /f: <filename>    полное имя файла, в который будут выводиться данные (по умолчанию rnd.dat)')
    print('  /i: <params>      перечисление параметров для выбранного генератора')

def main():
    args = sys.argv[1:]
    method = None
    n = 10000
    filename = 'rnd.dat'

    for arg in args:
        if arg.startswith('/g:'):
            method = arg[3:]
        elif arg.startswith('/n:'):
            n = int(arg[3:])
        elif arg.startswith('/f:'):
            filename = arg[3:]
        elif arg.startswith("/i:"):
            input_args = arg[3:]
        elif arg == '/h':
            if arg != args[0]:
                print('Ошибка: /h не может быть использован одновременно с другими аргументами!')
            print_usage()
            return

```



```

        else:
            print_help()
            return

if method is None:
    print('Метод не указан!')
    print_usage()
    return

elif input_args is None:
    print('Неуказаны аргументы для функций!')
    print_usage()
    return

random_numbers = generate_pseudo_random(method, input_args, n)

if random_numbers == []:
    return
else:
    with open(filename, 'w', encoding = 'UTF-8') as f:
        f.write(','.join(map(str, random_numbers)))
    print(f'Числа сгенерированы и сохранены в файл {filename}!')

if __name__ == '__main__':
    main()

```