МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

кафедра «Вычислительная техника».

**Лабораторная работа №1 (вариант 5)**

**тема: «Изучение генераторов псевдослучайных последовательностей»**

по дисциплине: «Информационная безопасность и защита информации»

Выполнил:

студент 4 курса, гр. ИВТВМбд-41

Захарычев Никита Алексеевич.

Проверил:

доцент кафедры ВТ,

кандидат технических наук

Мартынов Антон Иванович.

г. Ульяновск, 2017

**Задание**

1. Изучить алгоритм работы генераторов псевдослучайных чисел (ГПЧ)

2. Реализовать приложение, которое позволяет генерировать псевдослучайную последовательность чисел четырьмя различными способами:

* С помощью генератора встроенного в язык программирования высокого уровня;
* С помощью встроенного криптографического генератора в криптопровайдер Windows;
* С помощью первого генератора реализованного согласно варианту задания;
* С помощью второго генератора реализованного согласно варианту задания.

3. Исследовать полученную последовательность на случайность с помощью методики NIST STS 4.

|  |  |
| --- | --- |
| Вариант | Схема генератора псевдослучайной последовательности |
| 5 | Генератор Стоп-Пошел + Генератор Парка-Миллера |

**Описание используемых алгоритмов реализации генераторов**

#### Генератор «Стоп-пошел»

Этот генератор использует выход одного LFSR для управления тактовой частотой другого LFSR. Тактовый выход LFSR-2 управляется выходом LFSR-1, так что LFSR-2 может изменять свое состояние в момент времени *t* только, если выход LFSR-1 в момент времени *t–1* был равен *1 (Рис.1)*.

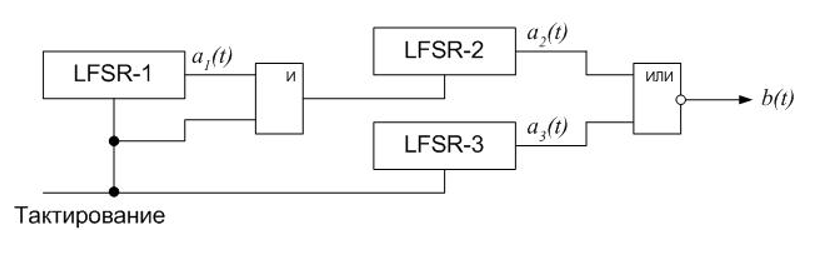


Рисунок . Генератор Стоп-Пошел

### Генератор Парка-Миллера

Самая простая последовательность, которую можно предложить для реализации генератора равномерного распределения:

**I(j+1)=a\*I(j)(mod m)**

при соответствующем выборе констант. Константы были предложены Park и Miller:

**a=75=16807, m=231-1=2147483647**

и протестированы в исследованиях Lewis, Goodman, Miller (1969).

Прямое приложение этого метода возможно на языках ассемблера, но языки высокого уровня могут при этом зафиксировать переполнение. Для обхода этого Scharge предложил метод частичной факторизации модуля. Модуль разлагается в выражение:

**m=a\*q+r**

Если r<q и 0<z<m-1, то при этом величины a\*(z mod q) и r\*[z/q] всегда лежат в интервале 0,...,m-1. Для умножения (a\*z)(mod m) при этом используется алгоритм:

* t = a(z mod q)-r[z/q]
* если t<0, то t += m.
* (a\*z)(mod m)=t.

В случае констант Парка-Миллера можно использовать q=12773 и r=2836.

**Отчет по результатам анализа каждого генератора**

1. **Генератор встроенный в язык программирования высокого уровня**

------------------------------------------------------------------------------

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

------------------------------------------------------------------------------

generator is <output>

------------------------------------------------------------------------------

C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 P-VALUE PROPORTION STATISTICAL TEST

------------------------------------------------------------------------------

8 10 8 10 20 10 9 11 6 8 0.162606 1.0000 Frequency

8 15 8 16 10 12 5 7 12 7 0.213309 1.0000 BlockFrequency

5 11 12 9 13 9 15 11 10 5 0.419021 0.9800 CumulativeSums

9 8 11 13 16 7 9 10 11 6 0.554420 1.0000 CumulativeSums

7 13 8 18 5 8 12 9 7 13 0.129620 0.9900 Runs

6 14 10 11 4 13 13 8 12 9 0.383827 1.0000 LongestRun

10 12 5 4 19 10 12 8 8 12 0.062821 1.0000 Rank

2 5 8 7 14 16 18 15 3 12 0.000513 1.0000 FFT

10 6 12 11 9 13 14 10 6 9 0.699313 1.0000 NonOverlappingTemplate

7 11 11 8 15 9 13 8 8 10 0.759756 0.9800 NonOverlappingTemplate

17 8 6 12 12 6 12 10 10 7 0.304126 0.9900 NonOverlappingTemplate

6 13 5 18 10 7 10 12 11 8 0.153763 1.0000 NonOverlappingTemplate

6 15 4 12 13 8 14 9 13 6 0.137282 0.9900 NonOverlappingTemplate

10 10 7 6 7 15 10 10 10 15 0.494392 1.0000 NonOverlappingTemplate

11 12 10 7 10 13 7 11 7 12 0.867692 0.9800 NonOverlappingTemplate

8 11 9 9 10 13 11 13 3 13 0.494392 0.9900 NonOverlappingTemplate

10 12 15 13 6 5 9 10 13 7 0.366918 1.0000 NonOverlappingTemplate

7 15 6 7 9 12 12 9 8 15 0.366918 1.0000 NonOverlappingTemplate

10 11 10 8 12 10 6 10 14 9 0.897763 1.0000 NonOverlappingTemplate

11 8 10 14 9 8 10 9 8 13 0.911413 0.9700 NonOverlappingTemplate

9 14 8 8 11 10 8 10 12 10 0.946308 1.0000 NonOverlappingTemplate

9 7 9 13 13 14 13 4 8 10 0.401199 0.9900 NonOverlappingTemplate

12 12 12 6 14 9 10 10 9 6 0.719747 0.9800 NonOverlappingTemplate

4 12 9 11 11 11 9 10 13 10 0.798139 1.0000 NonOverlappingTemplate

11 6 11 9 15 9 16 10 4 9 0.224821 0.9900 NonOverlappingTemplate

12 9 7 5 11 14 14 11 9 8 0.554420 0.9800 NonOverlappingTemplate

17 10 6 9 11 6 13 8 9 11 0.366918 1.0000 NonOverlappingTemplate

6 10 11 9 13 10 6 9 10 16 0.534146 0.9800 NonOverlappingTemplate

8 14 10 8 8 8 9 13 11 11 0.883171 0.9800 NonOverlappingTemplate

15 5 9 16 11 10 7 9 8 10 0.334538 0.9800 NonOverlappingTemplate

9 11 17 10 11 6 12 7 9 8 0.474986 0.9900 NonOverlappingTemplate

9 13 12 9 8 6 7 17 8 11 0.366918 1.0000 NonOverlappingTemplate

6 8 9 11 12 11 14 9 9 11 0.867692 1.0000 NonOverlappingTemplate

11 11 9 9 11 10 11 12 6 10 0.978072 0.9900 NonOverlappingTemplate

8 10 6 7 12 15 11 14 9 8 0.534146 0.9800 NonOverlappingTemplate

10 8 11 9 10 4 14 8 16 10 0.366918 0.9700 NonOverlappingTemplate

8 12 11 12 13 8 4 9 13 10 0.616305 1.0000 NonOverlappingTemplate

10 8 11 10 11 8 8 8 17 9 0.657933 1.0000 NonOverlappingTemplate

10 11 11 10 10 14 11 10 7 6 0.883171 0.9900 NonOverlappingTemplate

9 14 9 9 12 3 12 8 8 16 0.213309 1.0000 NonOverlappingTemplate

8 8 12 7 13 10 16 5 12 9 0.383827 0.9800 NonOverlappingTemplate

10 9 9 14 8 8 11 15 7 9 0.719747 0.9800 NonOverlappingTemplate

7 14 7 9 11 11 10 7 11 13 0.779188 0.9900 NonOverlappingTemplate

11 10 6 8 11 10 10 12 11 11 0.971699 1.0000 NonOverlappingTemplate

8 10 7 11 15 13 10 5 11 10 0.595549 0.9900 NonOverlappingTemplate

6 11 12 13 11 6 10 8 13 10 0.739918 0.9900 NonOverlappingTemplate

8 6 9 10 17 13 14 6 6 11 0.171867 0.9900 NonOverlappingTemplate

9 6 11 4 10 6 16 13 16 9 0.085587 1.0000 NonOverlappingTemplate

8 9 13 8 4 16 7 12 8 15 0.153763 0.9900 NonOverlappingTemplate

19 10 10 5 12 10 11 6 7 10 0.137282 0.9800 NonOverlappingTemplate

7 9 10 14 12 9 6 10 9 14 0.699313 1.0000 NonOverlappingTemplate

14 10 10 9 8 7 9 13 7 13 0.759756 0.9700 NonOverlappingTemplate

8 9 10 6 20 9 9 14 7 8 0.085587 1.0000 NonOverlappingTemplate

12 10 13 12 6 10 10 12 5 10 0.719747 0.9800 NonOverlappingTemplate

9 10 10 16 8 6 11 15 10 5 0.289667 1.0000 NonOverlappingTemplate

10 12 12 7 10 11 13 6 9 10 0.883171 0.9900 NonOverlappingTemplate

10 8 16 11 7 7 6 15 10 10 0.350485 0.9700 NonOverlappingTemplate

9 5 9 17 11 9 12 9 10 9 0.494392 1.0000 NonOverlappingTemplate

11 12 6 11 13 16 6 5 13 7 0.181557 0.9900 NonOverlappingTemplate

7 11 10 15 9 9 12 8 17 2 0.071177 0.9900 NonOverlappingTemplate

8 10 10 14 12 12 8 10 9 7 0.897763 0.9900 NonOverlappingTemplate

11 8 13 10 15 6 7 7 11 12 0.554420 0.9900 NonOverlappingTemplate

12 7 10 10 9 11 10 13 9 9 0.978072 0.9800 NonOverlappingTemplate

14 8 12 11 9 10 7 9 10 10 0.935716 0.9900 NonOverlappingTemplate

7 8 10 7 14 9 10 15 9 11 0.678686 0.9900 NonOverlappingTemplate

12 8 10 7 17 10 9 8 11 8 0.574903 0.9800 NonOverlappingTemplate

11 8 7 9 10 14 8 10 18 5 0.191687 1.0000 NonOverlappingTemplate

9 7 7 9 11 10 12 13 10 12 0.924076 1.0000 NonOverlappingTemplate

10 6 15 9 10 10 8 15 9 8 0.574903 1.0000 NonOverlappingTemplate

11 11 13 9 7 9 11 4 11 14 0.574903 0.9900 NonOverlappingTemplate

9 13 6 8 15 8 8 9 13 11 0.595549 1.0000 NonOverlappingTemplate

4 5 10 12 15 12 5 12 13 12 0.137282 1.0000 NonOverlappingTemplate

11 4 11 12 7 14 13 9 15 4 0.129620 0.9800 NonOverlappingTemplate

12 9 12 8 7 1 19 9 12 11 0.025193 0.9800 NonOverlappingTemplate

8 11 15 7 13 6 13 9 9 9 0.574903 1.0000 NonOverlappingTemplate

10 10 12 7 10 12 6 11 15 7 0.657933 0.9900 NonOverlappingTemplate

9 14 10 8 6 11 9 13 10 10 0.851383 0.9800 NonOverlappingTemplate

10 10 10 7 13 10 6 12 9 13 0.851383 0.9700 NonOverlappingTemplate

10 14 10 5 8 16 9 11 10 7 0.419021 0.9900 NonOverlappingTemplate

13 6 15 10 9 9 12 11 8 7 0.637119 0.9900 NonOverlappingTemplate

14 17 8 5 10 12 9 11 8 6 0.213309 0.9900 NonOverlappingTemplate

12 14 7 7 13 8 14 5 9 11 0.401199 0.9900 NonOverlappingTemplate

10 6 12 11 9 13 14 10 6 9 0.699313 1.0000 NonOverlappingTemplate

13 10 7 11 14 8 13 4 8 12 0.419021 0.9900 NonOverlappingTemplate

7 8 12 16 12 9 5 9 12 10 0.455937 0.9800 NonOverlappingTemplate

9 12 14 6 13 12 10 9 6 9 0.657933 0.9900 NonOverlappingTemplate

10 11 5 11 10 16 6 9 11 11 0.514124 0.9900 NonOverlappingTemplate

8 8 12 18 13 6 10 9 8 8 0.275709 1.0000 NonOverlappingTemplate

14 13 10 12 7 10 12 6 10 6 0.595549 0.9900 NonOverlappingTemplate

14 12 9 13 7 7 10 11 10 7 0.759756 1.0000 NonOverlappingTemplate

8 5 14 7 14 17 6 10 9 10 0.137282 0.9800 NonOverlappingTemplate

12 6 15 4 9 12 12 12 9 9 0.383827 0.9800 NonOverlappingTemplate

13 8 7 9 10 6 16 10 14 7 0.350485 0.9900 NonOverlappingTemplate

6 13 14 10 8 8 13 10 9 9 0.739918 0.9700 NonOverlappingTemplate

9 7 12 8 10 7 12 17 9 9 0.514124 0.9900 NonOverlappingTemplate

9 9 11 8 13 8 10 10 12 10 0.983453 1.0000 NonOverlappingTemplate

16 7 11 9 10 12 13 6 10 6 0.419021 0.9800 NonOverlappingTemplate

13 9 12 16 11 7 9 5 12 6 0.304126 1.0000 NonOverlappingTemplate

9 14 2 9 11 14 7 10 10 14 0.191687 0.9900 NonOverlappingTemplate

8 8 14 16 11 7 13 8 7 8 0.383827 0.9900 NonOverlappingTemplate

10 15 13 9 4 12 7 8 13 9 0.366918 0.9800 NonOverlappingTemplate

5 12 8 17 14 7 10 11 9 7 0.224821 1.0000 NonOverlappingTemplate

9 9 9 11 12 12 12 12 9 5 0.867692 1.0000 NonOverlappingTemplate

14 9 13 12 9 9 12 5 2 15 0.090936 0.9900 NonOverlappingTemplate

14 15 9 9 8 5 7 11 15 7 0.236810 1.0000 NonOverlappingTemplate

9 11 6 10 7 16 14 9 10 8 0.494392 0.9900 NonOverlappingTemplate

9 6 10 14 10 13 4 10 10 14 0.401199 0.9800 NonOverlappingTemplate

14 14 8 10 14 7 5 10 8 10 0.437274 0.9700 NonOverlappingTemplate

9 10 10 14 9 13 10 9 7 9 0.924076 0.9900 NonOverlappingTemplate

6 14 7 10 13 13 11 12 8 6 0.494392 0.9900 NonOverlappingTemplate

13 15 10 10 13 3 9 7 10 10 0.334538 1.0000 NonOverlappingTemplate

15 3 11 7 12 11 13 11 8 9 0.319084 1.0000 NonOverlappingTemplate

12 14 10 8 9 11 10 6 12 8 0.834308 0.9900 NonOverlappingTemplate

5 10 13 11 10 10 6 12 10 13 0.699313 0.9900 NonOverlappingTemplate

10 13 14 12 7 12 8 6 6 12 0.514124 1.0000 NonOverlappingTemplate

5 9 12 7 6 11 13 13 11 13 0.494392 1.0000 NonOverlappingTemplate

5 8 14 13 11 10 10 12 13 4 0.319084 0.9900 NonOverlappingTemplate

6 12 11 8 14 9 14 6 11 9 0.574903 1.0000 NonOverlappingTemplate

8 10 10 13 11 12 8 5 11 12 0.816537 0.9900 NonOverlappingTemplate

11 6 15 10 10 10 14 10 11 3 0.289667 0.9900 NonOverlappingTemplate

16 11 8 8 14 8 7 8 9 11 0.534146 1.0000 NonOverlappingTemplate

14 12 10 5 5 9 8 10 11 16 0.262249 0.9900 NonOverlappingTemplate

9 9 9 11 10 10 11 12 7 12 0.987896 1.0000 NonOverlappingTemplate

10 9 6 10 9 13 6 3 13 21 0.008266 1.0000 NonOverlappingTemplate

12 18 10 10 12 12 11 7 2 6 0.055361 1.0000 NonOverlappingTemplate

12 16 8 12 7 7 7 8 12 11 0.494392 0.9800 NonOverlappingTemplate

11 6 8 11 17 9 11 9 8 10 0.554420 1.0000 NonOverlappingTemplate

10 13 4 6 14 12 12 13 5 11 0.213309 1.0000 NonOverlappingTemplate

9 14 11 7 7 13 9 11 9 10 0.851383 0.9800 NonOverlappingTemplate

9 12 7 12 10 11 5 14 13 7 0.554420 1.0000 NonOverlappingTemplate

12 11 4 14 12 16 7 8 10 6 0.181557 0.9900 NonOverlappingTemplate

11 12 11 9 8 13 11 9 6 10 0.924076 0.9900 NonOverlappingTemplate

7 7 8 10 7 4 10 20 12 15 0.020548 0.9900 NonOverlappingTemplate

8 13 7 8 14 7 13 11 13 6 0.474986 0.9900 NonOverlappingTemplate

11 12 7 7 10 7 11 8 12 15 0.678686 0.9900 NonOverlappingTemplate

11 8 10 10 8 14 10 10 5 14 0.678686 0.9800 NonOverlappingTemplate

9 8 10 5 14 17 7 11 7 12 0.224821 1.0000 NonOverlappingTemplate

11 11 10 6 8 10 11 11 9 13 0.946308 0.9800 NonOverlappingTemplate

7 13 11 12 3 10 9 9 11 15 0.350485 1.0000 NonOverlappingTemplate

7 10 10 11 5 8 13 16 11 9 0.474986 1.0000 NonOverlappingTemplate

12 8 14 11 11 8 8 10 6 12 0.798139 0.9800 NonOverlappingTemplate

12 10 15 7 8 6 10 12 12 8 0.637119 0.9900 NonOverlappingTemplate

15 6 12 7 11 9 10 9 7 14 0.514124 0.9900 NonOverlappingTemplate

7 11 16 10 14 5 10 9 10 8 0.419021 1.0000 NonOverlappingTemplate

8 7 6 16 8 14 12 12 9 8 0.366918 0.9800 NonOverlappingTemplate

10 7 11 11 6 9 11 12 12 11 0.924076 0.9800 NonOverlappingTemplate

10 12 12 6 7 13 10 9 11 10 0.883171 0.9800 NonOverlappingTemplate

6 9 17 7 12 12 6 12 9 10 0.319084 0.9900 NonOverlappingTemplate

8 6 8 15 8 5 9 14 10 17 0.108791 0.9900 NonOverlappingTemplate

9 10 17 6 8 9 9 14 8 10 0.419021 0.9900 NonOverlappingTemplate

5 11 7 14 4 10 14 7 17 11 0.062821 0.9800 NonOverlappingTemplate

9 12 12 11 14 6 7 9 10 10 0.816537 0.9900 NonOverlappingTemplate

11 4 8 12 5 17 15 6 13 9 0.048716 0.9900 NonOverlappingTemplate

6 9 9 12 8 13 11 11 11 10 0.924076 1.0000 NonOverlappingTemplate

8 9 10 6 12 7 10 9 14 15 0.574903 0.9800 NonOverlappingTemplate

12 14 7 7 13 8 15 4 9 11 0.249284 0.9900 NonOverlappingTemplate

12 15 9 12 7 10 10 8 9 8 0.816537 0.9900 OverlappingTemplate

11 11 10 10 11 9 11 7 14 6 0.867692 0.9800 Universal

13 16 7 5 10 9 11 7 6 16 0.115387 0.9500 \* ApproximateEntropy

8 9 9 5 10 7 3 7 4 5 0.422034 0.9552 \* RandomExcursions

11 12 8 4 7 5 3 7 5 5 0.128379 0.9851 RandomExcursions

8 13 5 5 6 9 8 3 5 5 0.155209 1.0000 RandomExcursions

9 5 8 7 9 9 6 4 8 2 0.392456 0.9851 RandomExcursions

10 4 11 8 8 6 2 7 6 5 0.222869 1.0000 RandomExcursions

5 5 6 12 10 7 6 5 5 6 0.392456 0.9851 RandomExcursions

8 9 10 7 8 7 4 2 5 7 0.392456 1.0000 RandomExcursions

3 5 7 5 11 4 10 6 6 10 0.204076 1.0000 RandomExcursions

11 6 10 7 2 8 5 3 10 5 0.095617 0.9851 RandomExcursionsVariant

9 10 11 4 6 4 8 7 5 3 0.204076 0.9851 RandomExcursionsVariant

9 10 9 4 6 7 5 6 4 7 0.585209 0.9701 RandomExcursionsVariant

9 5 9 8 6 4 9 6 5 6 0.723129 0.9851 RandomExcursionsVariant

8 5 10 7 6 1 7 8 6 9 0.337162 1.0000 RandomExcursionsVariant

8 10 6 4 4 4 11 6 9 5 0.264458 0.9851 RandomExcursionsVariant

9 9 6 6 5 8 6 3 11 4 0.337162 0.9851 RandomExcursionsVariant

9 6 12 7 5 7 7 6 6 2 0.287306 0.9701 RandomExcursionsVariant

9 8 5 7 6 13 3 5 4 7 0.155209 0.9552 \* RandomExcursionsVariant

9 3 6 5 8 7 3 4 7 15 0.018969 0.9851 RandomExcursionsVariant

8 10 4 8 4 5 5 4 7 12 0.186566 0.9851 RandomExcursionsVariant

5 12 4 5 8 3 10 8 7 5 0.170294 1.0000 RandomExcursionsVariant

5 9 4 5 5 6 11 7 7 8 0.551026 1.0000 RandomExcursionsVariant

5 8 4 10 6 9 5 5 8 7 0.654467 1.0000 RandomExcursionsVariant

4 9 4 9 10 6 6 4 11 4 0.186566 1.0000 RandomExcursionsVariant

4 9 5 9 9 6 6 4 10 5 0.452799 1.0000 RandomExcursionsVariant

3 6 10 6 9 14 1 1 8 9 0.001490 1.0000 RandomExcursionsVariant

1 9 7 4 11 9 7 8 5 6 0.155209 1.0000 RandomExcursionsVariant

12 12 8 14 8 7 13 11 4 11 0.455937 0.9700 Serial

10 12 13 7 8 12 11 9 6 12 0.816537 0.9900 Serial

8 12 7 11 10 16 7 11 6 12 0.494392 1.0000 LinearComplexity

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

The minimum pass rate for each statistical test with the exception of the

random excursion (variant) test is approximately = 0.960150 for a

sample size = 100 binary sequences.

The minimum pass rate for the random excursion (variant) test

is approximately 0.953533 for a sample size = 67 binary sequences.

For further guidelines construct a probability table using the MAPLE program

provided in the addendum section of the documentation.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

1. **Встроенный криптографический генератор в криптопровайдер Windows**

------------------------------------------------------------------------------

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

------------------------------------------------------------------------------

generator is <output>

------------------------------------------------------------------------------

C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 P-VALUE PROPORTION STATISTICAL TEST

------------------------------------------------------------------------------

17 12 8 9 9 11 8 5 10 11 0.437274 0.9800 Frequency

14 9 8 10 6 14 12 8 6 13 0.474986 0.9600 BlockFrequency

12 17 11 7 4 9 12 10 10 8 0.289667 0.9800 CumulativeSums

14 14 5 10 12 3 14 7 13 8 0.096578 0.9800 CumulativeSums

9 11 10 10 9 13 9 13 6 10 0.924076 1.0000 Runs

10 13 12 6 9 10 7 13 13 7 0.678686 0.9800 LongestRun

3 12 11 10 7 13 6 14 11 13 0.249284 0.9900 Rank

4 5 8 11 10 13 12 16 13 8 0.171867 1.0000 FFT

7 11 8 15 10 12 2 16 10 9 0.108791 1.0000 NonOverlappingTemplate

9 14 7 7 12 11 13 11 8 8 0.759756 0.9900 NonOverlappingTemplate

14 8 7 10 9 12 9 10 10 11 0.935716 1.0000 NonOverlappingTemplate

11 15 6 8 9 11 10 7 15 8 0.474986 0.9700 NonOverlappingTemplate

9 12 7 10 7 18 8 10 11 8 0.383827 0.9900 NonOverlappingTemplate

7 3 9 12 14 11 11 12 12 9 0.437274 0.9900 NonOverlappingTemplate

9 12 9 14 4 12 8 11 12 9 0.616305 0.9900 NonOverlappingTemplate

14 9 8 12 9 10 10 11 6 11 0.883171 0.9900 NonOverlappingTemplate

10 7 10 15 10 12 6 9 8 13 0.657933 1.0000 NonOverlappingTemplate

13 8 12 9 13 16 5 4 12 8 0.153763 0.9900 NonOverlappingTemplate

8 11 11 5 9 15 11 11 12 7 0.616305 1.0000 NonOverlappingTemplate

14 7 9 12 16 8 3 9 9 13 0.162606 0.9800 NonOverlappingTemplate

9 6 9 14 13 11 10 5 8 15 0.366918 0.9900 NonOverlappingTemplate

6 5 18 6 8 14 10 13 13 7 0.051942 1.0000 NonOverlappingTemplate

9 5 7 14 13 12 9 6 9 16 0.224821 0.9600 NonOverlappingTemplate

10 7 10 13 6 7 9 15 12 11 0.595549 1.0000 NonOverlappingTemplate

9 12 11 5 5 11 11 14 13 9 0.494392 1.0000 NonOverlappingTemplate

16 11 10 10 11 10 7 5 4 16 0.108791 0.9700 NonOverlappingTemplate

11 8 12 14 12 9 8 4 8 14 0.437274 0.9800 NonOverlappingTemplate

11 8 11 13 8 15 6 11 11 6 0.554420 0.9500 \* NonOverlappingTemplate

12 8 12 11 8 6 11 8 12 12 0.867692 1.0000 NonOverlappingTemplate

7 12 8 13 10 5 11 11 12 11 0.759756 0.9900 NonOverlappingTemplate

6 9 10 12 10 10 14 7 13 9 0.779188 1.0000 NonOverlappingTemplate

10 7 10 9 11 13 11 11 12 6 0.897763 0.9800 NonOverlappingTemplate

6 12 5 10 9 10 7 10 18 13 0.171867 1.0000 NonOverlappingTemplate

9 5 11 5 7 15 12 10 15 11 0.236810 1.0000 NonOverlappingTemplate

13 13 7 10 11 8 11 11 8 8 0.897763 0.9900 NonOverlappingTemplate

9 15 9 5 8 12 18 7 11 6 0.090936 1.0000 NonOverlappingTemplate

9 17 6 13 8 15 6 6 11 9 0.129620 0.9800 NonOverlappingTemplate

11 9 7 10 11 10 11 11 7 13 0.955835 0.9900 NonOverlappingTemplate

12 9 11 5 15 11 12 11 8 6 0.514124 0.9900 NonOverlappingTemplate

12 7 7 10 15 12 9 11 8 9 0.759756 0.9800 NonOverlappingTemplate

13 5 12 9 15 7 9 11 9 10 0.574903 0.9700 NonOverlappingTemplate

11 3 14 10 7 10 12 8 12 13 0.383827 0.9800 NonOverlappingTemplate

6 7 12 10 10 12 14 9 12 8 0.759756 0.9900 NonOverlappingTemplate

7 4 15 17 4 6 13 16 8 10 0.008879 0.9800 NonOverlappingTemplate

17 6 10 13 7 8 7 11 12 9 0.334538 0.9900 NonOverlappingTemplate

12 11 7 10 14 12 11 12 7 4 0.494392 0.9900 NonOverlappingTemplate

14 11 11 10 11 12 7 10 9 5 0.759756 0.9900 NonOverlappingTemplate

12 5 13 10 7 13 6 10 14 10 0.455937 0.9900 NonOverlappingTemplate

12 13 10 6 11 12 6 13 9 8 0.699313 0.9900 NonOverlappingTemplate

7 15 4 12 11 13 15 6 11 6 0.115387 1.0000 NonOverlappingTemplate

5 13 13 8 9 7 13 11 10 11 0.657933 0.9900 NonOverlappingTemplate

14 12 4 14 11 8 12 12 7 6 0.275709 1.0000 NonOverlappingTemplate

7 10 9 8 12 8 16 9 11 10 0.739918 1.0000 NonOverlappingTemplate

8 5 13 10 12 12 16 9 8 7 0.383827 0.9800 NonOverlappingTemplate

8 14 4 5 11 10 14 11 12 11 0.319084 1.0000 NonOverlappingTemplate

9 7 10 13 16 8 7 8 14 8 0.419021 0.9900 NonOverlappingTemplate

7 10 7 14 14 13 8 11 10 6 0.534146 1.0000 NonOverlappingTemplate

10 14 5 7 12 14 12 6 12 8 0.366918 0.9900 NonOverlappingTemplate

9 15 10 14 14 7 8 5 13 5 0.162606 0.9900 NonOverlappingTemplate

12 10 11 7 10 5 7 14 14 10 0.534146 0.9900 NonOverlappingTemplate

11 16 10 13 10 8 6 5 11 10 0.419021 1.0000 NonOverlappingTemplate

7 14 10 12 15 10 6 12 11 3 0.191687 1.0000 NonOverlappingTemplate

10 14 9 10 11 9 14 4 12 7 0.494392 0.9900 NonOverlappingTemplate

12 14 14 7 7 7 8 5 15 11 0.224821 0.9800 NonOverlappingTemplate

14 9 9 9 8 9 11 14 8 9 0.867692 0.9800 NonOverlappingTemplate

12 4 13 13 10 4 11 12 10 11 0.350485 0.9900 NonOverlappingTemplate

6 9 8 13 11 10 11 8 10 14 0.816537 1.0000 NonOverlappingTemplate

16 7 11 9 11 10 9 7 11 9 0.739918 0.9800 NonOverlappingTemplate

13 3 12 9 12 6 11 6 19 9 0.032923 0.9900 NonOverlappingTemplate

9 7 12 16 5 7 11 12 8 13 0.334538 1.0000 NonOverlappingTemplate

6 11 5 10 15 7 14 11 14 7 0.224821 1.0000 NonOverlappingTemplate

10 13 9 9 13 13 7 10 10 6 0.798139 1.0000 NonOverlappingTemplate

11 9 7 7 8 13 11 9 12 13 0.851383 0.9900 NonOverlappingTemplate

9 3 10 16 11 14 7 11 9 10 0.249284 0.9900 NonOverlappingTemplate

11 8 12 10 10 11 4 10 9 15 0.616305 0.9900 NonOverlappingTemplate

14 11 10 10 6 10 4 14 10 11 0.474986 0.9800 NonOverlappingTemplate

11 7 10 13 13 13 4 6 16 7 0.145326 0.9800 NonOverlappingTemplate

12 16 5 10 12 8 10 13 7 7 0.350485 1.0000 NonOverlappingTemplate

5 10 12 9 16 9 6 12 11 10 0.455937 1.0000 NonOverlappingTemplate

11 15 5 8 9 9 9 7 17 10 0.236810 1.0000 NonOverlappingTemplate

10 9 10 11 10 9 12 10 8 11 0.998821 0.9800 NonOverlappingTemplate

10 14 10 16 8 5 6 11 11 9 0.350485 0.9900 NonOverlappingTemplate

7 12 7 15 10 12 2 16 10 9 0.085587 1.0000 NonOverlappingTemplate

11 7 6 8 10 17 8 11 10 12 0.455937 0.9800 NonOverlappingTemplate

16 11 10 7 8 14 10 7 14 3 0.122325 0.9900 NonOverlappingTemplate

11 10 13 9 9 10 14 9 7 8 0.897763 0.9900 NonOverlappingTemplate

7 13 14 9 9 10 7 10 12 9 0.834308 0.9900 NonOverlappingTemplate

5 8 9 9 12 11 9 12 14 11 0.759756 0.9900 NonOverlappingTemplate

9 17 8 9 8 12 8 8 9 12 0.574903 0.9800 NonOverlappingTemplate

11 13 14 13 8 9 7 10 13 2 0.202268 1.0000 NonOverlappingTemplate

11 13 9 9 10 12 9 7 8 12 0.946308 0.9500 \* NonOverlappingTemplate

7 6 13 8 10 9 13 8 8 18 0.213309 0.9800 NonOverlappingTemplate

13 11 4 11 15 12 7 9 12 6 0.304126 0.9900 NonOverlappingTemplate

12 14 14 12 13 9 5 7 9 5 0.275709 0.9800 NonOverlappingTemplate

6 12 9 9 9 8 13 4 12 18 0.122325 1.0000 NonOverlappingTemplate

10 6 9 11 12 12 8 14 11 7 0.779188 1.0000 NonOverlappingTemplate

2 10 9 7 10 9 7 14 20 12 0.015598 1.0000 NonOverlappingTemplate

10 9 8 13 5 15 14 6 8 12 0.319084 0.9800 NonOverlappingTemplate

10 11 11 6 9 12 12 11 10 8 0.955835 1.0000 NonOverlappingTemplate

9 7 10 12 12 8 8 12 12 10 0.946308 1.0000 NonOverlappingTemplate

12 10 5 9 14 8 8 9 13 12 0.657933 1.0000 NonOverlappingTemplate

12 5 7 14 17 10 12 8 8 7 0.191687 1.0000 NonOverlappingTemplate

11 14 5 10 11 15 12 8 9 5 0.334538 0.9900 NonOverlappingTemplate

8 9 8 17 9 13 10 9 11 6 0.474986 0.9900 NonOverlappingTemplate

13 10 10 6 13 9 13 7 11 8 0.759756 0.9800 NonOverlappingTemplate

17 8 8 13 8 7 12 9 12 6 0.319084 0.9700 NonOverlappingTemplate

10 9 8 7 11 13 11 13 13 5 0.657933 1.0000 NonOverlappingTemplate

10 4 11 13 14 8 10 11 7 12 0.534146 0.9900 NonOverlappingTemplate

11 16 8 9 7 12 14 5 10 8 0.350485 1.0000 NonOverlappingTemplate

10 15 9 10 13 10 14 8 5 6 0.383827 1.0000 NonOverlappingTemplate

9 9 11 13 7 10 11 15 7 8 0.739918 0.9800 NonOverlappingTemplate

13 15 8 6 10 21 4 5 10 8 0.004301 0.9900 NonOverlappingTemplate

9 7 15 10 7 9 4 11 11 17 0.153763 0.9900 NonOverlappingTemplate

12 12 6 14 6 12 9 12 9 8 0.637119 1.0000 NonOverlappingTemplate

9 12 11 13 10 6 9 7 9 14 0.759756 1.0000 NonOverlappingTemplate

12 9 14 11 5 11 9 7 9 13 0.657933 0.9600 NonOverlappingTemplate

15 9 12 5 7 10 8 7 11 16 0.249284 1.0000 NonOverlappingTemplate

9 7 9 12 13 9 11 8 10 12 0.946308 1.0000 NonOverlappingTemplate

9 5 10 14 10 15 7 10 9 11 0.554420 1.0000 NonOverlappingTemplate

9 5 6 14 10 10 14 9 13 10 0.494392 0.9900 NonOverlappingTemplate

8 15 13 8 12 10 7 9 11 7 0.678686 0.9900 NonOverlappingTemplate

15 10 12 7 11 11 9 6 9 10 0.759756 1.0000 NonOverlappingTemplate

13 9 16 11 7 13 8 3 8 12 0.181557 0.9700 NonOverlappingTemplate

8 12 10 7 12 6 6 13 13 13 0.534146 1.0000 NonOverlappingTemplate

12 8 7 10 9 4 18 11 8 13 0.153763 0.9700 NonOverlappingTemplate

6 14 8 14 15 8 8 9 11 7 0.383827 0.9800 NonOverlappingTemplate

13 18 5 11 8 10 7 11 6 11 0.162606 1.0000 NonOverlappingTemplate

16 15 4 8 9 6 8 10 10 14 0.129620 0.9600 NonOverlappingTemplate

7 11 15 6 8 7 15 10 8 13 0.334538 1.0000 NonOverlappingTemplate

13 6 11 17 10 9 9 8 9 8 0.474986 0.9800 NonOverlappingTemplate

16 7 11 10 10 9 11 8 10 8 0.779188 0.9900 NonOverlappingTemplate

9 7 10 17 12 10 9 8 8 10 0.616305 1.0000 NonOverlappingTemplate

12 4 9 14 12 14 7 8 8 12 0.366918 1.0000 NonOverlappingTemplate

10 9 12 5 12 10 12 10 8 12 0.867692 1.0000 NonOverlappingTemplate

11 8 10 9 8 15 12 10 7 10 0.851383 0.9900 NonOverlappingTemplate

9 9 7 11 6 15 14 11 8 10 0.595549 1.0000 NonOverlappingTemplate

6 8 10 3 14 21 12 7 8 11 0.007694 1.0000 NonOverlappingTemplate

9 8 7 11 12 11 9 11 8 14 0.897763 1.0000 NonOverlappingTemplate

19 12 9 14 10 7 7 10 7 5 0.080519 0.9900 NonOverlappingTemplate

6 6 15 14 14 9 8 14 8 6 0.162606 0.9900 NonOverlappingTemplate

12 10 10 12 13 5 9 7 9 13 0.719747 0.9800 NonOverlappingTemplate

7 10 10 7 7 15 11 6 11 16 0.304126 1.0000 NonOverlappingTemplate

13 7 13 9 14 3 11 8 12 10 0.334538 0.9700 NonOverlappingTemplate

6 10 5 11 8 12 11 9 9 19 0.145326 0.9900 NonOverlappingTemplate

10 7 14 9 7 15 9 7 10 12 0.595549 0.9800 NonOverlappingTemplate

7 7 9 8 11 15 10 8 16 9 0.437274 0.9900 NonOverlappingTemplate

11 4 18 9 7 9 11 8 15 8 0.102526 0.9900 NonOverlappingTemplate

5 12 7 14 13 11 9 9 10 10 0.678686 1.0000 NonOverlappingTemplate

13 8 7 15 10 12 9 12 7 7 0.595549 0.9900 NonOverlappingTemplate

6 16 14 9 4 13 12 7 13 6 0.085587 0.9900 NonOverlappingTemplate

6 16 11 7 13 10 10 6 11 10 0.455937 0.9900 NonOverlappingTemplate

10 12 12 6 8 10 9 8 12 13 0.867692 0.9700 NonOverlappingTemplate

6 15 8 11 8 11 10 11 10 10 0.816537 0.9900 NonOverlappingTemplate

8 13 6 9 8 9 17 12 9 9 0.437274 1.0000 NonOverlappingTemplate

13 10 14 15 12 7 8 7 9 5 0.334538 0.9900 NonOverlappingTemplate

10 14 10 16 8 5 6 11 11 9 0.350485 0.9900 NonOverlappingTemplate

8 9 13 17 6 7 13 5 12 10 0.181557 0.9900 OverlappingTemplate

12 11 7 7 9 8 15 8 12 11 0.719747 0.9900 Universal

11 4 5 16 9 14 10 11 10 10 0.236810 0.9900 ApproximateEntropy

4 5 6 3 7 6 4 8 8 8 0.554420 1.0000 RandomExcursions

5 6 9 6 8 6 6 5 4 4 0.719747 1.0000 RandomExcursions

2 4 5 7 11 8 5 3 7 7 0.115387 1.0000 RandomExcursions

2 6 5 8 7 6 8 7 7 3 0.437274 1.0000 RandomExcursions

5 5 8 6 3 6 5 8 7 6 0.759756 1.0000 RandomExcursions

3 8 4 9 6 6 8 6 5 4 0.474986 0.9831 RandomExcursions

5 7 7 3 4 5 4 7 10 7 0.401199 1.0000 RandomExcursions

10 5 4 6 6 3 8 7 2 8 0.181557 0.9492 \* RandomExcursions

6 3 5 7 5 6 7 6 6 8 0.834308 0.9831 RandomExcursionsVariant

6 5 5 5 4 4 4 10 7 9 0.366918 1.0000 RandomExcursionsVariant

7 4 6 4 3 3 5 9 9 9 0.181557 1.0000 RandomExcursionsVariant

5 7 2 6 2 5 7 7 9 9 0.181557 1.0000 RandomExcursionsVariant

5 6 5 3 6 7 2 11 5 9 0.115387 1.0000 RandomExcursionsVariant

7 6 3 5 2 10 13 3 5 5 0.008266 0.9831 RandomExcursionsVariant

8 6 2 7 3 5 8 3 11 6 0.080519 0.9661 RandomExcursionsVariant

6 11 1 3 6 7 6 6 8 5 0.102526 0.9661 RandomExcursionsVariant

8 4 6 6 8 2 5 5 8 7 0.474986 0.9831 RandomExcursionsVariant

7 8 6 7 11 4 3 3 5 5 0.181557 0.9831 RandomExcursionsVariant

5 9 12 8 5 2 5 5 2 6 0.028817 0.9831 RandomExcursionsVariant

4 7 9 7 7 6 5 5 3 6 0.637119 1.0000 RandomExcursionsVariant

5 9 3 6 7 8 8 5 6 2 0.304126 1.0000 RandomExcursionsVariant

4 8 3 5 9 8 10 3 6 3 0.102526 1.0000 RandomExcursionsVariant

3 7 7 5 4 8 10 7 3 5 0.275709 0.9831 RandomExcursionsVariant

3 5 6 8 2 10 10 3 3 9 0.021999 0.9831 RandomExcursionsVariant

3 4 8 4 2 11 7 9 5 6 0.062821 1.0000 RandomExcursionsVariant

2 6 9 4 5 11 6 5 5 6 0.162606 1.0000 RandomExcursionsVariant

10 7 11 10 9 11 13 12 7 10 0.946308 1.0000 Serial

9 10 8 9 11 13 5 12 11 12 0.834308 0.9800 Serial

16 11 8 9 10 13 6 12 8 7 0.494392 0.9700 LinearComplexity

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

The minimum pass rate for each statistical test with the exception of the

random excursion (variant) test is approximately = 0.960150 for a

sample size = 100 binary sequences.

The minimum pass rate for the random excursion (variant) test

is approximately 0.951139 for a sample size = 59 binary sequences.

For further guidelines construct a probability table using the MAPLE program

provided in the addendum section of the documentation.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

1. **Генератор Стоп-Пошел**

*------------------------------------------------------------------------------*

*RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES*

*------------------------------------------------------------------------------*

*generator is <output>*

*------------------------------------------------------------------------------*

*C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 P-VALUE PROPORTION STATISTICAL TEST*

*------------------------------------------------------------------------------*

*24 8 9 11 9 6 10 5 11 7 0.002559 0.9100 \* Frequency*

*4 0 5 3 2 4 4 8 18 52 0.000000 \* 1.0000 BlockFrequency*

*24 10 13 13 11 7 6 8 5 3 0.000216 0.9000 \* CumulativeSums*

*24 15 12 10 9 7 14 2 6 1 0.000005 \* 0.9100 \* CumulativeSums*

*100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0200 \* Runs*

*72 10 3 5 5 2 2 1 0 0 0.000000 \* 0.6700 \* LongestRun*

*7 12 9 11 10 13 14 7 12 5 0.554420 0.9800 Rank*

*4 5 5 8 7 12 14 13 18 14 0.013569 1.0000 FFT*

*41 14 7 8 6 5 6 4 7 2 0.000000 \* 0.8800 \* NonOverlappingTemplate*

*29 12 8 15 9 6 5 8 3 5 0.000000 \* 0.9600 NonOverlappingTemplate*

*13 13 10 16 9 11 3 12 8 5 0.129620 0.9800 NonOverlappingTemplate*

*18 14 8 9 10 14 13 5 3 6 0.017912 0.9800 NonOverlappingTemplate*

*16 12 10 13 10 11 7 8 5 8 0.419021 0.9900 NonOverlappingTemplate*

*16 8 7 15 14 8 4 11 8 9 0.137282 1.0000 NonOverlappingTemplate*

*5 10 10 15 5 9 7 10 16 13 0.162606 0.9800 NonOverlappingTemplate*

*30 13 19 6 9 6 8 5 3 1 0.000000 \* 0.9400 \* NonOverlappingTemplate*

*12 14 9 13 9 11 9 8 9 6 0.798139 0.9900 NonOverlappingTemplate*

*10 8 6 15 13 9 9 8 11 11 0.719747 0.9800 NonOverlappingTemplate*

*11 13 10 7 4 9 5 12 20 9 0.028817 0.9900 NonOverlappingTemplate*

*7 16 11 10 9 11 10 10 10 6 0.699313 0.9800 NonOverlappingTemplate*

*8 9 15 12 12 2 11 9 11 11 0.304126 0.9900 NonOverlappingTemplate*

*12 12 7 8 11 8 13 12 9 8 0.883171 0.9900 NonOverlappingTemplate*

*7 6 11 8 10 15 11 13 10 9 0.678686 0.9800 NonOverlappingTemplate*

*20 17 12 11 11 2 12 6 6 3 0.000375 0.9700 NonOverlappingTemplate*

*8 17 11 3 7 8 15 9 14 8 0.062821 0.9800 NonOverlappingTemplate*

*12 14 11 6 7 7 10 10 14 9 0.616305 0.9800 NonOverlappingTemplate*

*9 5 10 14 10 10 8 13 10 11 0.779188 1.0000 NonOverlappingTemplate*

*7 17 7 9 10 13 16 5 10 6 0.080519 0.9900 NonOverlappingTemplate*

*12 5 11 15 11 12 9 10 6 9 0.554420 0.9900 NonOverlappingTemplate*

*13 11 13 11 12 6 7 13 8 6 0.554420 0.9700 NonOverlappingTemplate*

*9 13 6 15 8 7 16 11 8 7 0.249284 0.9800 NonOverlappingTemplate*

*7 15 14 10 4 10 11 7 14 8 0.236810 1.0000 NonOverlappingTemplate*

*9 8 10 12 19 11 6 11 6 8 0.171867 0.9800 NonOverlappingTemplate*

*8 9 10 15 8 11 3 11 15 10 0.275709 0.9900 NonOverlappingTemplate*

*8 12 10 8 11 10 9 7 15 10 0.851383 1.0000 NonOverlappingTemplate*

*4 15 9 14 8 8 12 10 10 10 0.437274 1.0000 NonOverlappingTemplate*

*12 6 11 12 8 13 9 9 9 11 0.897763 1.0000 NonOverlappingTemplate*

*24 13 13 14 11 5 6 8 2 4 0.000021 \* 0.9500 \* NonOverlappingTemplate*

*8 15 9 7 8 13 12 6 12 10 0.574903 1.0000 NonOverlappingTemplate*

*7 9 15 12 9 8 11 16 2 11 0.102526 0.9800 NonOverlappingTemplate*

*11 9 11 11 9 10 7 11 11 10 0.996335 0.9700 NonOverlappingTemplate*

*15 9 9 9 14 10 6 17 3 8 0.062821 0.9600 NonOverlappingTemplate*

*18 10 11 12 5 8 9 10 10 7 0.289667 0.9900 NonOverlappingTemplate*

*7 4 16 12 12 12 12 8 13 4 0.102526 1.0000 NonOverlappingTemplate*

*14 11 11 12 9 9 7 10 7 10 0.897763 1.0000 NonOverlappingTemplate*

*17 11 11 11 12 8 8 10 8 4 0.319084 0.9400 \* NonOverlappingTemplate*

*13 15 4 15 8 5 11 16 6 7 0.028817 0.9900 NonOverlappingTemplate*

*14 10 12 15 16 9 6 6 5 7 0.096578 0.9800 NonOverlappingTemplate*

*20 9 7 9 7 11 7 11 11 8 0.137282 0.9600 NonOverlappingTemplate*

*12 11 15 12 9 8 6 11 7 9 0.678686 0.9700 NonOverlappingTemplate*

*17 11 13 12 7 6 6 12 6 10 0.191687 0.9900 NonOverlappingTemplate*

*8 11 14 11 13 14 7 10 6 6 0.455937 1.0000 NonOverlappingTemplate*

*11 16 10 8 12 9 8 10 8 8 0.759756 0.9700 NonOverlappingTemplate*

*17 13 6 5 9 7 11 12 11 9 0.236810 0.9900 NonOverlappingTemplate*

*7 13 5 11 10 11 18 13 8 4 0.071177 1.0000 NonOverlappingTemplate*

*19 6 13 7 11 11 11 9 9 4 0.075719 0.9400 \* NonOverlappingTemplate*

*7 14 6 8 14 10 8 8 12 13 0.514124 0.9900 NonOverlappingTemplate*

*13 6 12 14 14 10 7 5 5 14 0.137282 0.9800 NonOverlappingTemplate*

*13 10 14 5 11 13 5 8 8 13 0.334538 0.9900 NonOverlappingTemplate*

*26 16 11 8 15 6 6 6 4 2 0.000000 \* 0.9700 NonOverlappingTemplate*

*13 11 7 10 12 14 9 7 8 9 0.798139 0.9800 NonOverlappingTemplate*

*9 16 9 6 7 13 11 12 7 10 0.474986 0.9800 NonOverlappingTemplate*

*14 14 10 7 7 7 6 12 10 13 0.455937 0.9900 NonOverlappingTemplate*

*6 13 10 11 9 8 16 10 8 9 0.616305 1.0000 NonOverlappingTemplate*

*8 14 8 13 8 12 9 4 15 9 0.319084 0.9900 NonOverlappingTemplate*

*16 10 7 10 12 6 7 20 6 6 0.014550 0.9900 NonOverlappingTemplate*

*11 10 8 17 9 7 11 12 10 5 0.401199 0.9800 NonOverlappingTemplate*

*9 12 11 14 8 15 8 8 11 4 0.383827 1.0000 NonOverlappingTemplate*

*11 15 13 7 15 5 7 12 6 9 0.191687 0.9800 NonOverlappingTemplate*

*9 14 9 11 6 7 14 11 8 11 0.678686 0.9900 NonOverlappingTemplate*

*19 11 8 12 9 12 5 9 5 10 0.102526 0.9900 NonOverlappingTemplate*

*9 7 11 10 15 8 9 15 8 8 0.595549 0.9500 \* NonOverlappingTemplate*

*13 11 10 16 12 9 5 10 6 8 0.383827 0.9800 NonOverlappingTemplate*

*17 9 10 11 7 7 15 8 6 10 0.249284 0.9900 NonOverlappingTemplate*

*19 15 12 8 8 8 10 7 5 8 0.066882 0.9900 NonOverlappingTemplate*

*11 13 17 11 9 13 9 5 9 3 0.102526 0.9600 NonOverlappingTemplate*

*14 8 11 9 14 8 15 6 9 6 0.350485 0.9900 NonOverlappingTemplate*

*10 7 15 6 9 13 10 10 7 13 0.554420 0.9700 NonOverlappingTemplate*

*11 11 12 9 8 15 7 10 9 8 0.834308 0.9900 NonOverlappingTemplate*

*14 10 15 8 8 10 12 11 6 6 0.474986 1.0000 NonOverlappingTemplate*

*14 15 9 9 14 9 9 7 6 8 0.437274 0.9800 NonOverlappingTemplate*

*50 12 7 5 5 9 4 4 4 0 0.000000 \* 0.9200 \* NonOverlappingTemplate*

*41 14 7 8 6 5 6 4 7 2 0.000000 \* 0.8800 \* NonOverlappingTemplate*

*14 8 12 10 11 14 7 7 7 10 0.657933 0.9900 NonOverlappingTemplate*

*20 11 12 12 12 10 5 8 5 5 0.023545 0.9600 NonOverlappingTemplate*

*8 13 9 7 12 12 13 7 11 8 0.798139 0.9800 NonOverlappingTemplate*

*5 10 9 13 15 9 9 12 9 9 0.657933 0.9900 NonOverlappingTemplate*

*12 14 12 7 6 11 8 12 10 8 0.719747 0.9700 NonOverlappingTemplate*

*16 13 11 17 9 10 6 2 6 10 0.023545 0.9800 NonOverlappingTemplate*

*4 11 6 12 11 7 14 14 11 10 0.350485 1.0000 NonOverlappingTemplate*

*12 14 13 9 6 7 12 10 9 8 0.699313 0.9600 NonOverlappingTemplate*

*14 5 14 8 7 9 9 14 12 8 0.383827 0.9800 NonOverlappingTemplate*

*18 9 8 11 10 10 5 9 10 10 0.383827 0.9900 NonOverlappingTemplate*

*14 14 12 9 9 6 14 13 5 4 0.122325 0.9700 NonOverlappingTemplate*

*12 8 10 12 12 15 11 6 8 6 0.554420 0.9800 NonOverlappingTemplate*

*16 5 8 13 12 13 11 7 9 6 0.249284 0.9800 NonOverlappingTemplate*

*6 8 12 11 13 13 12 8 7 10 0.739918 0.9900 NonOverlappingTemplate*

*15 14 10 15 12 6 7 7 10 4 0.122325 0.9900 NonOverlappingTemplate*

*10 8 11 9 20 3 6 9 11 13 0.032923 0.9900 NonOverlappingTemplate*

*22 12 10 9 9 4 10 6 7 11 0.011791 0.9300 \* NonOverlappingTemplate*

*8 9 8 18 7 11 10 10 12 7 0.383827 0.9900 NonOverlappingTemplate*

*7 16 11 13 5 10 9 13 9 7 0.350485 0.9800 NonOverlappingTemplate*

*9 9 8 7 11 10 8 14 9 15 0.719747 0.9900 NonOverlappingTemplate*

*7 9 10 13 8 13 14 11 10 5 0.595549 1.0000 NonOverlappingTemplate*

*26 14 21 11 10 3 8 3 2 2 0.000000 \* 0.9600 NonOverlappingTemplate*

*12 11 11 6 11 8 17 10 10 4 0.262249 0.9900 NonOverlappingTemplate*

*9 12 14 8 18 7 8 11 9 4 0.122325 1.0000 NonOverlappingTemplate*

*7 11 8 10 8 7 17 10 12 10 0.534146 1.0000 NonOverlappingTemplate*

*15 17 13 4 14 5 10 10 8 4 0.017912 0.9600 NonOverlappingTemplate*

*14 7 11 9 11 13 4 7 20 4 0.009535 0.9800 NonOverlappingTemplate*

*17 10 13 7 9 12 6 8 11 7 0.334538 0.9700 NonOverlappingTemplate*

*17 10 8 5 13 12 8 13 6 8 0.191687 0.9800 NonOverlappingTemplate*

*14 6 12 17 4 20 10 5 7 5 0.000954 0.9900 NonOverlappingTemplate*

*15 14 8 6 10 11 11 10 6 9 0.534146 0.9700 NonOverlappingTemplate*

*12 5 14 9 4 13 7 15 11 10 0.181557 0.9900 NonOverlappingTemplate*

*10 6 11 7 11 11 7 14 14 9 0.637119 1.0000 NonOverlappingTemplate*

*10 10 8 10 10 13 11 8 12 8 0.978072 0.9800 NonOverlappingTemplate*

*15 12 4 12 12 8 9 11 12 5 0.289667 0.9700 NonOverlappingTemplate*

*21 10 9 7 13 9 9 4 8 10 0.032923 0.9700 NonOverlappingTemplate*

*12 13 14 9 11 10 6 10 9 6 0.699313 0.9800 NonOverlappingTemplate*

*9 15 7 10 11 12 6 11 12 7 0.637119 1.0000 NonOverlappingTemplate*

*7 11 9 18 9 10 13 8 7 8 0.334538 0.9800 NonOverlappingTemplate*

*13 11 15 14 6 6 7 7 12 9 0.304126 0.9800 NonOverlappingTemplate*

*10 13 11 7 6 15 8 12 3 15 0.115387 0.9700 NonOverlappingTemplate*

*10 15 10 14 14 9 6 12 6 4 0.162606 0.9800 NonOverlappingTemplate*

*8 12 11 12 12 12 7 13 7 6 0.699313 1.0000 NonOverlappingTemplate*

*26 18 12 8 8 5 7 8 4 4 0.000001 \* 0.9800 NonOverlappingTemplate*

*6 10 14 13 14 10 10 9 9 5 0.494392 1.0000 NonOverlappingTemplate*

*13 14 11 9 10 10 7 13 6 7 0.637119 1.0000 NonOverlappingTemplate*

*18 8 11 8 9 12 7 15 3 9 0.062821 0.9600 NonOverlappingTemplate*

*11 7 7 9 17 8 11 9 9 12 0.534146 0.9900 NonOverlappingTemplate*

*14 14 11 7 13 5 6 6 13 11 0.224821 0.9700 NonOverlappingTemplate*

*6 12 8 9 13 12 18 5 10 7 0.137282 0.9900 NonOverlappingTemplate*

*8 10 10 11 6 11 9 13 11 11 0.946308 1.0000 NonOverlappingTemplate*

*15 9 9 9 10 16 9 8 6 9 0.474986 0.9700 NonOverlappingTemplate*

*16 10 4 4 9 12 13 10 7 15 0.075719 0.9800 NonOverlappingTemplate*

*20 12 9 10 9 4 9 11 7 9 0.080519 0.9400 \* NonOverlappingTemplate*

*12 11 11 7 11 13 6 11 7 11 0.816537 1.0000 NonOverlappingTemplate*

*15 10 9 7 12 9 8 7 13 10 0.719747 0.9900 NonOverlappingTemplate*

*12 10 11 11 9 13 11 9 9 5 0.883171 1.0000 NonOverlappingTemplate*

*18 17 17 10 8 9 8 6 4 3 0.001296 0.9800 NonOverlappingTemplate*

*8 9 11 13 11 11 8 7 10 12 0.946308 0.9900 NonOverlappingTemplate*

*10 13 8 10 6 5 19 8 11 10 0.122325 0.9900 NonOverlappingTemplate*

*10 10 7 7 11 11 16 11 7 10 0.678686 0.9900 NonOverlappingTemplate*

*4 10 13 10 8 14 12 12 10 7 0.514124 1.0000 NonOverlappingTemplate*

*11 8 8 12 7 12 8 14 11 9 0.851383 0.9700 NonOverlappingTemplate*

*17 10 10 6 8 11 15 6 4 13 0.075719 0.9800 NonOverlappingTemplate*

*10 8 16 15 11 4 13 7 6 10 0.137282 0.9900 NonOverlappingTemplate*

*21 16 11 10 7 10 7 6 6 6 0.007694 0.9800 NonOverlappingTemplate*

*10 12 8 11 10 8 12 10 6 13 0.897763 0.9900 NonOverlappingTemplate*

*14 8 21 12 9 9 8 7 5 7 0.021999 1.0000 NonOverlappingTemplate*

*16 8 10 7 12 15 8 8 10 6 0.334538 0.9700 NonOverlappingTemplate*

*18 21 13 11 8 8 8 6 5 2 0.000274 0.9700 NonOverlappingTemplate*

*16 12 12 12 10 8 8 11 3 8 0.275709 0.9700 NonOverlappingTemplate*

*30 22 10 9 8 9 3 4 4 1 0.000000 \* 0.9800 NonOverlappingTemplate*

*50 11 8 5 5 9 4 4 4 0 0.000000 \* 0.9200 \* NonOverlappingTemplate*

*29 11 14 11 9 6 6 6 5 3 0.000000 \* 0.9300 \* OverlappingTemplate*

*0 0 100 0 0 0 0 0 0 0 0.000000 \* 1.0000 Universal*

*42 18 17 6 6 4 4 0 2 1 0.000000 \* 0.9100 \* ApproximateEntropy*

*0 1 0 0 0 0 0 0 0 1 ---- 1.0000 RandomExcursions*

*1 0 0 0 0 0 0 0 0 1 ---- 1.0000 RandomExcursions*

*0 0 0 0 0 0 0 2 0 0 ---- 1.0000 RandomExcursions*

*0 0 0 1 0 0 0 0 0 1 ---- 1.0000 RandomExcursions*

*0 0 0 0 0 0 2 0 0 0 ---- 1.0000 RandomExcursions*

*0 0 0 0 0 1 0 1 0 0 ---- 1.0000 RandomExcursions*

*0 0 0 0 0 1 0 0 1 0 ---- 1.0000 RandomExcursions*

*0 0 0 0 1 1 0 0 0 0 ---- 1.0000 RandomExcursions*

*0 0 1 0 0 0 0 0 1 0 ---- 1.0000 RandomExcursionsVariant*

*0 0 0 0 0 1 0 0 1 0 ---- 1.0000 RandomExcursionsVariant*

*0 0 0 0 0 0 1 1 0 0 ---- 1.0000 RandomExcursionsVariant*

*0 0 0 0 0 0 0 1 0 1 ---- 1.0000 RandomExcursionsVariant*

*0 0 0 0 0 0 0 1 1 0 ---- 1.0000 RandomExcursionsVariant*

*0 0 0 0 0 0 0 0 0 2 ---- 1.0000 RandomExcursionsVariant*

*0 0 0 0 0 0 0 0 0 2 ---- 1.0000 RandomExcursionsVariant*

*0 0 0 0 0 0 0 1 0 1 ---- 1.0000 RandomExcursionsVariant*

*0 0 0 0 1 0 0 0 1 0 ---- 1.0000 RandomExcursionsVariant*

*0 2 0 0 0 0 0 0 0 0 ---- 1.0000 RandomExcursionsVariant*

*0 0 1 0 1 0 0 0 0 0 ---- 1.0000 RandomExcursionsVariant*

*0 0 0 2 0 0 0 0 0 0 ---- 1.0000 RandomExcursionsVariant*

*0 1 0 1 0 0 0 0 0 0 ---- 1.0000 RandomExcursionsVariant*

*0 1 0 0 1 0 0 0 0 0 ---- 1.0000 RandomExcursionsVariant*

*1 0 0 0 0 1 0 0 0 0 ---- 1.0000 RandomExcursionsVariant*

*1 0 0 0 0 0 0 0 0 1 ---- 1.0000 RandomExcursionsVariant*

*1 0 0 0 0 0 1 0 0 0 ---- 1.0000 RandomExcursionsVariant*

*0 1 0 0 0 1 0 0 0 0 ---- 1.0000 RandomExcursionsVariant*

*16 10 11 16 7 8 8 6 9 9 0.289667 1.0000 Serial*

*14 4 11 11 11 9 7 11 14 8 0.474986 0.9800 Serial*

*8 13 9 10 11 12 8 9 10 10 0.983453 0.9900 LinearComplexity*

*- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*

*The minimum pass rate for each statistical test with the exception of the*

*random excursion (variant) test is approximately = 0.960150 for a*

*sample size = 100 binary sequences.*

*The minimum pass rate for the random excursion (variant) test*

*is approximately 0.778931 for a sample size = 2 binary sequences.*

*For further guidelines construct a probability table using the MAPLE program*

*provided in the addendum section of the documentation.*

*- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*

**4) Генератор Парка-Миллера**

------------------------------------------------------------------------------

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

------------------------------------------------------------------------------

generator is <output>

------------------------------------------------------------------------------

C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 P-VALUE PROPORTION STATISTICAL TEST

------------------------------------------------------------------------------

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* Frequency

65 13 8 4 3 3 0 3 1 0 0.000000 \* 0.7600 \* BlockFrequency

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* CumulativeSums

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* CumulativeSums

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* Runs

91 3 2 0 2 1 0 0 1 0 0.000000 \* 0.4200 \* LongestRun

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* Rank

92 7 0 1 0 0 0 0 0 0 0.000000 \* 0.5200 \* FFT

86 6 7 1 0 0 0 0 0 0 0.000000 \* 0.4400 \* NonOverlappingTemplate

15 11 20 6 11 9 6 2 9 11 0.007160 0.9800 NonOverlappingTemplate

89 5 3 1 0 1 1 0 0 0 0.000000 \* 0.3500 \* NonOverlappingTemplate

18 12 14 13 11 8 8 6 6 4 0.048716 0.9600 NonOverlappingTemplate

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0200 \* NonOverlappingTemplate

64 8 7 7 3 6 2 1 0 2 0.000000 \* 0.7000 \* NonOverlappingTemplate

70 15 5 5 1 0 2 0 1 1 0.000000 \* 0.6700 \* NonOverlappingTemplate

9 13 13 12 8 8 9 13 4 11 0.554420 1.0000 NonOverlappingTemplate

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* NonOverlappingTemplate

89 7 0 2 2 0 0 0 0 0 0.000000 \* 0.3900 \* NonOverlappingTemplate

87 7 1 3 2 0 0 0 0 0 0.000000 \* 0.4100 \* NonOverlappingTemplate

17 8 12 10 12 10 13 9 4 5 0.153763 0.9800 NonOverlappingTemplate

83 8 5 0 3 1 0 0 0 0 0.000000 \* 0.4500 \* NonOverlappingTemplate

16 11 16 10 6 13 8 7 5 8 0.122325 0.9900 NonOverlappingTemplate

10 12 13 9 12 16 7 6 6 9 0.383827 0.9900 NonOverlappingTemplate

25 15 9 10 8 9 10 4 7 3 0.000060 \* 0.9600 NonOverlappingTemplate

97 2 1 0 0 0 0 0 0 0 0.000000 \* 0.2600 \* NonOverlappingTemplate

95 2 1 2 0 0 0 0 0 0 0.000000 \* 0.3300 \* NonOverlappingTemplate

19 16 15 12 5 12 9 2 6 4 0.000600 0.9400 \* NonOverlappingTemplate

95 1 2 1 1 0 0 0 0 0 0.000000 \* 0.1800 \* NonOverlappingTemplate

23 12 13 12 10 5 6 6 4 9 0.000954 0.9700 NonOverlappingTemplate

23 17 12 9 6 8 11 6 3 5 0.000114 0.9800 NonOverlappingTemplate

19 17 13 9 9 4 8 4 9 8 0.008266 0.9900 NonOverlappingTemplate

20 11 14 17 11 7 7 2 7 4 0.000555 0.9800 NonOverlappingTemplate

19 17 15 12 10 5 6 7 5 4 0.001399 0.9600 NonOverlappingTemplate

17 14 17 12 9 6 8 5 7 5 0.019188 0.9900 NonOverlappingTemplate

25 11 8 13 13 9 5 5 5 6 0.000089 \* 0.9800 NonOverlappingTemplate

22 16 13 7 9 6 7 3 9 8 0.001030 0.9500 \* NonOverlappingTemplate

18 14 13 10 12 9 6 5 8 5 0.058984 0.9800 NonOverlappingTemplate

96 3 0 0 0 1 0 0 0 0 0.000000 \* 0.2900 \* NonOverlappingTemplate

94 5 0 1 0 0 0 0 0 0 0.000000 \* 0.1800 \* NonOverlappingTemplate

98 1 1 0 0 0 0 0 0 0 0.000000 \* 0.1800 \* NonOverlappingTemplate

25 15 13 13 8 7 5 5 5 4 0.000011 \* 0.9200 \* NonOverlappingTemplate

31 15 15 11 7 6 6 3 4 2 0.000000 \* 0.8900 \* NonOverlappingTemplate

21 23 9 11 6 7 9 3 6 5 0.000005 \* 0.9500 \* NonOverlappingTemplate

17 9 12 12 6 14 7 10 4 9 0.137282 0.9400 \* NonOverlappingTemplate

32 17 11 4 4 7 10 5 4 6 0.000000 \* 0.9100 \* NonOverlappingTemplate

27 26 10 5 8 6 9 1 5 3 0.000000 \* 0.9000 \* NonOverlappingTemplate

16 11 8 8 7 12 11 12 9 6 0.534146 0.9900 NonOverlappingTemplate

23 16 7 9 7 5 7 11 9 6 0.001112 0.9600 NonOverlappingTemplate

20 11 13 11 9 7 3 8 10 8 0.037566 0.9900 NonOverlappingTemplate

89 3 7 1 0 0 0 0 0 0 0.000000 \* 0.3200 \* NonOverlappingTemplate

32 14 10 10 7 9 4 4 6 4 0.000000 \* 0.9300 \* NonOverlappingTemplate

11 11 13 8 12 7 14 8 5 11 0.595549 0.9900 NonOverlappingTemplate

15 15 16 16 6 7 6 9 5 5 0.010988 0.9900 NonOverlappingTemplate

14 14 12 8 15 9 7 7 9 5 0.275709 0.9800 NonOverlappingTemplate

91 4 1 1 0 1 1 1 0 0 0.000000 \* 0.4200 \* NonOverlappingTemplate

19 11 11 9 12 8 9 8 9 4 0.145326 0.9900 NonOverlappingTemplate

91 4 1 2 2 0 0 0 0 0 0.000000 \* 0.3400 \* NonOverlappingTemplate

94 6 0 0 0 0 0 0 0 0 0.000000 \* 0.3400 \* NonOverlappingTemplate

90 6 2 0 0 1 0 1 0 0 0.000000 \* 0.4200 \* NonOverlappingTemplate

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* NonOverlappingTemplate

98 1 0 0 1 0 0 0 0 0 0.000000 \* 0.1600 \* NonOverlappingTemplate

31 15 12 12 10 5 2 8 3 2 0.000000 \* 0.9600 NonOverlappingTemplate

36 18 12 6 3 9 7 4 3 2 0.000000 \* 0.9200 \* NonOverlappingTemplate

20 12 9 8 8 6 12 5 9 11 0.066882 0.9900 NonOverlappingTemplate

38 14 10 9 6 7 4 4 5 3 0.000000 \* 0.8600 \* NonOverlappingTemplate

15 10 10 15 7 7 7 15 6 8 0.202268 0.9900 NonOverlappingTemplate

16 9 13 5 12 10 12 7 12 4 0.171867 0.9900 NonOverlappingTemplate

86 7 3 1 2 1 0 0 0 0 0.000000 \* 0.3900 \* NonOverlappingTemplate

37 14 5 7 11 4 6 7 7 2 0.000000 \* 0.9000 \* NonOverlappingTemplate

10 14 8 10 11 8 6 10 11 12 0.867692 0.9700 NonOverlappingTemplate

18 12 12 9 9 15 5 4 6 10 0.040108 0.9800 NonOverlappingTemplate

90 5 1 1 3 0 0 0 0 0 0.000000 \* 0.4400 \* NonOverlappingTemplate

9 16 8 10 8 12 7 11 10 9 0.739918 0.9800 NonOverlappingTemplate

85 8 2 2 1 0 2 0 0 0 0.000000 \* 0.4300 \* NonOverlappingTemplate

89 6 3 1 1 0 0 0 0 0 0.000000 \* 0.4600 \* NonOverlappingTemplate

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* NonOverlappingTemplate

10 9 8 15 8 10 12 8 6 14 0.595549 0.9700 NonOverlappingTemplate

78 8 7 2 1 2 2 0 0 0 0.000000 \* 0.5100 \* NonOverlappingTemplate

86 6 1 4 2 1 0 0 0 0 0.000000 \* 0.3900 \* NonOverlappingTemplate

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0100 \* NonOverlappingTemplate

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* NonOverlappingTemplate

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* NonOverlappingTemplate

86 6 7 1 0 0 0 0 0 0 0.000000 \* 0.4400 \* NonOverlappingTemplate

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* NonOverlappingTemplate

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0100 \* NonOverlappingTemplate

94 2 2 2 0 0 0 0 0 0 0.000000 \* 0.2700 \* NonOverlappingTemplate

84 7 2 2 3 1 1 0 0 0 0.000000 \* 0.4500 \* NonOverlappingTemplate

28 19 14 11 5 8 3 5 3 4 0.000000 \* 0.9300 \* NonOverlappingTemplate

91 4 2 1 1 0 1 0 0 0 0.000000 \* 0.3600 \* NonOverlappingTemplate

95 2 2 1 0 0 0 0 0 0 0.000000 \* 0.1800 \* NonOverlappingTemplate

93 5 0 1 0 0 0 0 1 0 0.000000 \* 0.2800 \* NonOverlappingTemplate

26 15 8 12 6 8 5 5 9 6 0.000021 \* 0.9100 \* NonOverlappingTemplate

88 7 2 2 0 1 0 0 0 0 0.000000 \* 0.4000 \* NonOverlappingTemplate

22 15 16 11 7 7 6 7 6 3 0.000253 0.9400 \* NonOverlappingTemplate

25 12 12 12 8 10 7 4 6 4 0.000097 \* 0.9200 \* NonOverlappingTemplate

11 15 17 8 8 10 9 5 9 8 0.249284 0.9900 NonOverlappingTemplate

66 11 9 2 6 4 1 1 0 0 0.000000 \* 0.6100 \* NonOverlappingTemplate

38 12 12 8 14 4 2 3 4 3 0.000000 \* 0.9300 \* NonOverlappingTemplate

27 16 7 5 9 5 5 10 12 4 0.000001 \* 0.9200 \* NonOverlappingTemplate

11 16 12 15 7 9 9 7 5 9 0.262249 0.9900 NonOverlappingTemplate

22 11 13 10 8 9 8 4 6 9 0.010237 0.9500 \* NonOverlappingTemplate

18 7 8 10 4 15 12 8 11 7 0.075719 0.9900 NonOverlappingTemplate

15 17 10 5 15 11 6 4 10 7 0.028817 0.9800 NonOverlappingTemplate

98 2 0 0 0 0 0 0 0 0 0.000000 \* 0.3100 \* NonOverlappingTemplate

7 13 14 13 8 11 13 10 6 5 0.366918 0.9900 NonOverlappingTemplate

94 4 0 2 0 0 0 0 0 0 0.000000 \* 0.2100 \* NonOverlappingTemplate

97 0 1 1 1 0 0 0 0 0 0.000000 \* 0.2200 \* NonOverlappingTemplate

97 3 0 0 0 0 0 0 0 0 0.000000 \* 0.1800 \* NonOverlappingTemplate

36 15 7 10 6 7 4 7 5 3 0.000000 \* 0.9000 \* NonOverlappingTemplate

90 6 1 1 2 0 0 0 0 0 0.000000 \* 0.3900 \* NonOverlappingTemplate

38 21 4 13 4 4 4 3 6 3 0.000000 \* 0.8700 \* NonOverlappingTemplate

24 18 8 15 10 8 7 4 2 4 0.000002 \* 0.9400 \* NonOverlappingTemplate

30 12 11 8 8 8 6 4 6 7 0.000000 \* 0.9600 NonOverlappingTemplate

18 15 9 9 11 11 7 6 7 7 0.137282 0.9500 \* NonOverlappingTemplate

73 8 8 2 2 4 2 0 1 0 0.000000 \* 0.6300 \* NonOverlappingTemplate

33 18 12 11 4 2 8 4 4 4 0.000000 \* 0.9100 \* NonOverlappingTemplate

34 12 13 11 5 5 6 6 3 5 0.000000 \* 0.9300 \* NonOverlappingTemplate

22 15 8 13 10 8 8 5 8 3 0.001509 0.9700 NonOverlappingTemplate

12 12 17 12 11 6 8 5 9 8 0.262249 0.9900 NonOverlappingTemplate

15 11 8 9 10 7 12 11 12 5 0.595549 0.9900 NonOverlappingTemplate

22 14 7 11 6 9 5 10 7 9 0.008266 0.9400 \* NonOverlappingTemplate

14 9 5 15 4 8 13 10 9 13 0.181557 0.9900 NonOverlappingTemplate

19 12 9 8 5 8 9 14 9 7 0.102526 0.9800 NonOverlappingTemplate

35 17 6 7 8 7 4 3 6 7 0.000000 \* 0.9100 \* NonOverlappingTemplate

83 8 4 3 2 0 0 0 0 0 0.000000 \* 0.3700 \* NonOverlappingTemplate

87 9 1 2 0 1 0 0 0 0 0.000000 \* 0.4400 \* NonOverlappingTemplate

19 17 4 13 9 8 10 4 9 7 0.007160 0.9700 NonOverlappingTemplate

35 17 4 11 9 9 5 5 3 2 0.000000 \* 0.9100 \* NonOverlappingTemplate

37 24 3 10 3 6 2 5 8 2 0.000000 \* 0.9300 \* NonOverlappingTemplate

15 11 14 9 14 9 7 6 11 4 0.202268 0.9800 NonOverlappingTemplate

24 21 14 9 7 6 4 6 5 4 0.000000 \* 0.9300 \* NonOverlappingTemplate

12 10 9 13 14 14 9 10 2 7 0.213309 0.9800 NonOverlappingTemplate

12 10 17 10 12 10 12 6 6 5 0.224821 0.9900 NonOverlappingTemplate

18 17 11 15 10 6 5 9 6 3 0.003447 0.9700 NonOverlappingTemplate

8 15 7 8 9 8 15 12 9 9 0.554420 0.9900 NonOverlappingTemplate

21 15 13 11 10 7 5 9 6 3 0.002374 0.9500 \* NonOverlappingTemplate

79 10 3 2 2 0 2 1 1 0 0.000000 \* 0.5300 \* NonOverlappingTemplate

19 16 9 6 16 5 6 12 5 6 0.002374 1.0000 NonOverlappingTemplate

85 6 6 1 1 0 1 0 0 0 0.000000 \* 0.4300 \* NonOverlappingTemplate

90 6 1 2 0 0 1 0 0 0 0.000000 \* 0.2900 \* NonOverlappingTemplate

17 13 9 9 7 9 8 11 9 8 0.534146 0.9900 NonOverlappingTemplate

17 7 17 9 12 9 6 9 9 5 0.075719 0.9800 NonOverlappingTemplate

16 17 12 9 7 7 8 10 7 7 0.162606 1.0000 NonOverlappingTemplate

88 6 2 2 0 1 1 0 0 0 0.000000 \* 0.3600 \* NonOverlappingTemplate

17 11 14 9 14 6 11 4 9 5 0.062821 0.9800 NonOverlappingTemplate

89 5 1 3 0 0 2 0 0 0 0.000000 \* 0.3800 \* NonOverlappingTemplate

90 6 1 2 1 0 0 0 0 0 0.000000 \* 0.3800 \* NonOverlappingTemplate

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* NonOverlappingTemplate

24 26 17 8 6 5 6 2 2 4 0.000000 \* 0.9500 \* NonOverlappingTemplate

90 5 4 1 0 0 0 0 0 0 0.000000 \* 0.4100 \* NonOverlappingTemplate

87 5 2 2 3 0 0 1 0 0 0.000000 \* 0.4800 \* NonOverlappingTemplate

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* NonOverlappingTemplate

92 5 2 0 0 1 0 0 0 0 0.000000 \* 0.3500 \* NonOverlappingTemplate

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* NonOverlappingTemplate

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* NonOverlappingTemplate

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* NonOverlappingTemplate

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* OverlappingTemplate

23 6 10 9 6 7 10 11 4 14 0.001757 0.9700 Universal

100 0 0 0 0 0 0 0 0 0 0.000000 \* 0.0000 \* ApproximateEntropy

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursions

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursions

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursions

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursions

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursions

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursions

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursions

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursions

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

0 0 0 0 0 0 0 0 0 0 ---- ---- RandomExcursionsVariant

99 1 0 0 0 0 0 0 0 0 0.000000 \* 0.0600 \* Serial

18 12 7 9 16 14 5 4 6 9 0.013569 0.9500 \* Serial

16 7 7 7 7 9 10 7 15 15 0.153763 0.9900 LinearComplexity

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

The minimum pass rate for each statistical test with the exception of the

random excursion (variant) test is approximately = 0.960150 for a

sample size = 100 binary sequences.

The minimum pass rate for the random excursion (variant) test is undefined.

For further guidelines construct a probability table using the MAPLE program

provided in the addendum section of the documentation.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

**Исходный код**

using System;

using System.Collections.Generic;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

using System.IO;

using System.Security.Cryptography;

using System.Collections;

namespace ZashitaInf\_1

{

class Program

{

public static bool SaveToFile(string FileName, byte[] Data)

{

BinaryWriter Writer = null;

string Name = @"D:" + FileName;

try

{

Writer = new BinaryWriter(File.OpenWrite(Name));

Writer.Write(Data);

Writer.Flush();

Writer.Close();

}

catch

{

return false;

}

return true;

}

class GeneratorParkMiller

{

private long x0;

private const int a = 16807;

private const int m = 2147483647;

public GeneratorParkMiller(int num)

{

this.x0 = num;

}

public long[] getNexts(long len)

{

long[] arr = new long[len];

arr[0] = Random(this.x0);

for (int i = 1; i < arr.Length; i++)

{

arr[i] = Random(arr[i - 1]);

}

return arr;

}

public static byte[] getBytes(long len, long[] values)

{

var result = new List<byte>();

for (int i = 0; i < values.Length; i++)

{

byte[] tmp = BitConverter.GetBytes(values[i]);

for (int j = 0; j < tmp.Length; j++)

{

if (tmp[j] == 0) continue;

if (result.Count == len) return result.ToArray();

result.Add(tmp[j]);

}

}

return result.ToArray();

}

private long Random(long x) // рекурентное выражение

{

return (x \* a) % m;

}

}

public class LFSR

{

public int ShiftRegister { get; set; }

public int ShiftRegisterReserved { get; set; }

public int[] Polynomial { get; set; }

public Random r = new Random();

public LFSR(int value, int[] polynomial)

{

var r = new Random();

ShiftRegister = value;

ShiftRegisterReserved = r.Next();

this.Polynomial = polynomial;

}

public int GetBit()

{

if (ShiftRegister == 0 || ShiftRegister == Int32.MinValue)

ShiftRegister = r.Next();

int tmp = ShiftRegister;

for (int i = 0; i < Polynomial.Length; i++)

{

tmp ^= ShiftRegister >> (Polynomial[i] - 1);

}

tmp &= 0x00000001 << 31;

ShiftRegister = tmp | (ShiftRegister >> 1);

return ShiftRegister & 0x00000001;

}

}

class GenStopAndGo

{

public LFSR L1;

public LFSR L2;

public LFSR L3;

private Random rand = new Random();

public GenStopAndGo(int[] polinom1, int[] polinom2, int[] polinom3)

{

L1 = new LFSR(rand.Next(), polinom1);

L2 = new LFSR(rand.Next(), polinom2);

L3 = new LFSR(rand.Next(), polinom3);

}

public byte[] GetBytes(long length)

{

var result = new List<byte>();

for (int i = 0; i < length; i++)

{

string currentByte = "";

for (int j = 0; j < 8; j++)

{

currentByte += L1.GetBit() == 1 ? (L1.GetBit() & L2.GetBit()) : (L1.GetBit() & L3.GetBit());

}

result.Add(Convert.ToByte(currentByte, 2));

}

return result.ToArray();

}

}

static void Main(string[] args)

{

byte str = 0;

long len = 0;

Console.WriteLine("Лабораторная работа №1: Изучение генераторов псевдослучайных последовательностей");

Console.WriteLine("Выполнил: Захарычев Н.А \n");

Console.WriteLine("1. Встроенный генератор языка высокого уровня");

Console.WriteLine("2. Встроенный в криптопровайдер Windows криптографический генератор");

Console.WriteLine("3. Генератор Стоп-Пошел");

Console.WriteLine("4. Генератор Парка-Миллера \n");

while (str == 0)

{

Console.WriteLine("Введите начальное значение: ");

try

{

str = Byte.Parse(Console.ReadLine());

if (str == 0) throw new Exception();

} catch

{

Console.WriteLine("Неверное значение! Начальное значение должно быть в диапазоне от 1 до 255!");

}

}

while (len <= 0)

{

Console.WriteLine("Введите длину последовательности: ");

try

{

len = Int64.Parse(Console.ReadLine());

if (len <= 0) throw new Exception();

} catch

{

len = 0;

Console.WriteLine("Неверное значение! Длина может быть только целым положительным числом!");

}

}

byte[] sequence = new byte[len];

Console.WriteLine("Выберите генератор цифрой на клавиатуре: ");

ConsoleKeyInfo numKey = Console.ReadKey();

Console.WriteLine();

switch(numKey.Key)

{

case ConsoleKey.NumPad1:

{

Console.WriteLine("1. Встроенный генератор языка высокого уровня");

var stnd\_gen = new Random();

stnd\_gen.NextBytes(sequence);

break;

}

case ConsoleKey.NumPad2:

{

Console.WriteLine("2. Встроенный в криптопровайдер Windows криптографический генератор");

var win\_gen = new RNGCryptoServiceProvider();

win\_gen.GetBytes(sequence);

break;

}

case ConsoleKey.NumPad3:

{

Console.WriteLine("3. Генератор Стоп-Пошел");

int[] polinom1 = { 32, 7, 5, 3, 2, 1 };

int[] polinom2 = { 32, 7, 6, 2 };

int[] polinom3 = { 24, 4, 3, 1 };

var genstgo = new GenStopAndGo(polinom1, polinom2, polinom3);

sequence = genstgo.GetBytes(sequence.Length);

break;

}

case ConsoleKey.NumPad4:

{

Console.WriteLine("4. Генератор Парка-Миллера");

var GenParkMiller = new GeneratorParkMiller(str);

long[] arr = GenParkMiller.getNexts(sequence.Length);

sequence = GeneratorParkMiller.getBytes(sequence.Length, arr);

break;

}

default:

Console.WriteLine("Пожалуйста введите цифру от 1 до 4!");

Console.ReadKey();

break;

}

Console.WriteLine();

if (SaveToFile("output", sequence))

{

Console.WriteLine("Запись прошла успешно!");

}

else

{

Console.WriteLine("Ошибка записи!");

}

Console.WriteLine();

Console.ReadKey();

}

}

}