Лабораторная работа №4

Анализ криптографических качеств псевдослучайных последовательностей

Цель работы — исследовать криптографические качества некоторых генераторов гаммы путем тестирования псевдослучайных последовательностей, вырабатываемых генераторами.

Задания для каждого студента

1. Написать программу, реализующую заданный генератор гаммы.
2. Модифицировать написанную программу для проведения заданного типа тестирования последовательности, вырабатываемой генератором гаммы.
3. Сделать вывод о полученных результатах.

Индивидуальные задания

Индивидуальное задание для каждого студента представлено в приложении. Например, задание для студента Будницкого:

1) написать программу, реализующую *фильтрующий* генератор гаммы [1,2] с параметрами, приведенными в приложении;

2) модифицировать написанную программу с целью проведения теста *Discrete Fourier Transform (Spectral) Test* [3] последовательности, вырабатываемой реализованным генератором гаммы;

3) сделать вывод о криптографических качествах последовательности, вырабатываемой реализованным генератором гаммы.

Примечания

1. Во всех вариантах необходимо использовать ненулевые начальные состояния ЛРС.
2. Набором чисел (k,l,m) обозначен характеристический многочлен $f = 1 \oplus x^k \oplus x^l \oplus x^m$.

Список литературы

1. В. М. Фомичев. Методы дискретной математики в криптологии.
2. Б. Шнайер. Прикладная криптография.
3. NIST. A statistical test suite for random and pseudorandom number generators for cryptographic applications.

Приложение

№	Студент	Генератор	Параметры	Тест
1	**Будницкий**	Фильтрующий	ЛРС длины 30, характеристический мн-н: (1,4,6,30), фильтрующая ф-ция: $f = x_1x_9 \oplus x_{24}$	Discrete Fourier Transform (Spectral) Test
2	**Васильчиков**	Комбинирующий	m=3, характеристический мн-н ЛРС-1 длины 29: (2,29), характеристический мн-н ЛРС-2 длины 28: (3,28), характеристический мн-н ЛРС-3 длины 27: (1,2,5,27), комбинирующая ф-ция: $f = x_1x_2 \oplus x_3$	Non-overlapping Template Matching Test
3	**Власова**	Геффе	Характеристический мн-н ЛРС-1 длины 24: (1,2,7,24), характеристический мн-н ЛРС-2 длины 23: (5,23), характеристический мн-н ЛРС- 3 длины 19: (1,2,5,19)	Random Excursions Variant Test
4	**Вялов**	Пороговый	m=3, характеристический мн-н ЛРС-1 длины 19: (1,2,5,19), характеристический мн-н ЛРС-2 длины 18: (7,18), характеристический мн-н ЛРС- 3 длины 17: (3,17)	Test for the Longest Run of Ones in a Block
5	**Гинятуллин**	$(\delta,\tau)-$ самоусечения	$\delta = 2, \tau = 3$, характеристический мн-н ЛРС длины 30: (1,4,6,30), знак управляющей гаммы снимается с i-й ячейки регистра, i=11	Frequency Test within a Block
6	**Евтухин**	Сжимающий	Характеристический мн-н ЛРС-1 длины 14: (1,3,5,14), характеристический мн-н ЛРС-2 длины 13: (1,3,4,13)	Runs Test
7	**Зайцев**	С перемежающимся шагом	Характеристический мн-н ЛРС-1 длины 12: (1,4,8,12), характеристический мн-н ЛРС-2 длины 11: (2,11), характеристический мн-н ЛРС- 3 длины 10: (3,10), фильтрующая ф-ция: $f = x_3x_4 \oplus x_5 \oplus 1$	Binary Matrix Run Test
8	**Лазарев**	Стоп-вперед	Характеристический мн-н ЛРС-1 длины 29: (2,29), характеристический мн-н ЛРС-2 длины 23: (5,23), фильтрующая ф-ция: $f = x_5 \oplus x_{13}$	Discrete Fourier Transform (Spectral) Test
9	**Мельник**	ЛКГ	$x_{i+1} = (101x_i \oplus 25) \bmod 2^8, x_0 = 51$, построить двоичную выходную последовательность (элементы мн-ва представлять в виде элементов мн-ва V_8)	Non-overlapping Template Matching Test
10	**Мотрони**	$(\delta,\tau)-$ шагов	$\delta = 2, \tau = 3$, характеристический мн-н ЛРС-1 длины 19: (1,2,5,19), характеристический мн-н ЛРС-2 длины 18: (7,18), фильтрующая ф-ция: $f = x_2x_8 \oplus x_{15}$	Random Excursions Variant Test
11	**Музыченко**	A5/1	-	Test for the Longest Run of Ones in a Block
12	**Наумова**	Фильтрующий	ЛРС длины 29, характеристический мн-н: (2,29), фильтрующая ф-ция: $f = x_2x_4 \oplus x_6 \oplus 1$	Frequency Test within a Block
13	**Некоз**	Комбинирующий	m=3, характеристический мн-н ЛРС-1 длины 28: (3,28), характеристический мн-н ЛРС-2 длины 27: (1,2,5,27), характеристический мн-н ЛРС-3 длины 25: (3,25), комбинирующая ф-ция: $f = x_1 \oplus x_2 \oplus x_3$	Runs Test
14	**Писарев**	Геффе	Характеристический мн-н ЛРС-1 длины 23: (5,23), характеристический мн-н ЛРС-2 длины 22: (1,22), характеристический мн-н ЛРС- 3	Binary Matrix Run Test

№	Студент	Генератор	Параметры	Тест
			длины 21: (2,21)	
15	**Резвухин**	Пороговый	*m*=3, характеристический мн-н ЛРС-1 длины 18: (7,18), характеристический мн-н ЛРС-2 длины 17: (3,17), характеристический мн-н ЛРС- 3 длины 13: (1,3,4,13)	Discrete Fourier Transform (Spectral) Test
16	**Суходольский**	$(\delta,\tau)-$ самоусечения	$\delta=3,\tau=1$, характеристический мн-н ЛРС длины 31: (3,31), знак управляющей гаммы снимается с *i*-й ячейки регистра, *i*=12	Non-overlapping Template Matching Test
17	**Терехов**	Сжимающий	Характеристический мн-н ЛРС-1 длины 13: (1,3,4,13), характеристический мн-н ЛРС-2 длины 12: (1,4,8,12)	Random Excursions Variant Test
18	**Черников**	С перемежающимся шагом	Характеристический мн-н ЛРС-1 длины 16: (2,3,5,16), характеристический мн-н ЛРС-2 длины 15: (1,15), характеристический мн-н ЛРС- 3 длины 14: (1,3,5,14), фильтрующая ф-ция: $f=x_5x_7\oplus x_9$	Test for the Longest Run of Ones in a Block
19	**Шандер**	Стоп-вперед	Характеристический мн-н ЛРС-1 длины 28: (3,28), характеристический мн-н ЛРС-2 длины 22: (1,22), фильтрующая ф-ция: $f=x_{10}x_{11}\oplus x_{12}$	Frequency Test within a Block
20	**Шахов**	ЛКГ	$x_{i+1}=(105x_i\oplus 27)\bmod 2^8, x_0=52$, построить двоичную выходную последовательность (элементы мн-ва Z_{2^8} представлять в виде элементов мн-ва V_8)	Runs Test
21	**Шуйский**	$(\delta,\tau)-$ шагов	$d=3,t=1,$ характеристический мн-н ЛРС-1 длины 11: (2,11), характеристический мн-н ЛРС-2 длины 10: (3,10), фильтрующая ф-ция: $f=x_7\oplus x_9\oplus 1$	Binary Matrix Run Test
22	**Анисимов**	A5/1	-	Discrete Fourier Transform (Spectral) Test
23	**Антоненко**	Фильтрующий	ЛРС длины 28, характеристический мн-н: (3,28), фильтрующая ф-ция: $f=x_{19}x_{21}\oplus x_{23}$	Non-overlapping Template Matching Test
24	**Бондарев**	Комбинирующий	*m*=3, характеристический мн-н ЛРС-1 длины 27: (1,2,5,27), характеристический мн-н ЛРС-2 длины 26: (1,2,6,26), характеристический мн-н ЛРС-3 длины 25: (3,25), комбинирующая ф-ция: $f=x_1x_3\oplus x_2\oplus 1$	Random Excursions Variant Test
25	**Вантеев**	Геффе	Характеристический мн-н ЛРС-1 длины 22: (1,22), характеристический мн-н ЛРС-2 длины 21: (2,21), характеристический мн-н ЛРС- 3 длины 19: (1,2,5,19)	Test for the Longest Run of Ones in a Block
26	**Герасимов**	Пороговый	*m*=3, характеристический мн-н ЛРС-1 длины 17: (3,17), характеристический мн-н ЛРС-2 длины 16: (2,3,5,16), характеристический мн-н ЛРС- 3 длины 15: (1,15)	Frequency Test within a Block
27	**Деров**	$(\delta,\tau)-$ самоусечения	$\delta=3,\tau=2$, характеристический мн-н ЛРС длины 32: (1,2,22,32), знак управляющей гаммы снимается с *i*-й ячейки регистра, *i*=13	Runs Test
28	**Колесников**	Сжимающий	Характеристический мн-н ЛРС-1 длины 12: (1,4,8,12), характеристический мн-н ЛРС-2 длины 11: (2,11)	Binary Matrix Run Test
29	**Корнев**	С перемежающимся	Характеристический мн-н ЛРС-1 длины 22:	Discrete Fourier

№	Студент	Генератор	Параметры	Тест
		шагом	(1,22), характеристический мн-н ЛРС-2 длины 21: (2,21), характеристический мн-н ЛРС- 3 длины 20: (3,20), фильтрующая ф-ция: $f = x_{15}x_{17} \oplus x_{19} \oplus 1$	Transform (Spectral) Test
30	**Корчагин**	Стоп-вперед	Характеристический мн-н ЛРС-1 длины 27: (1,2,5,27), характеристический мн-н ЛРС-2 длины 21: (2,21), фильтрующая ф-ция: $f = x_3 \oplus x_{14}$	Non-overlapping Template Matching Test
31	**Ларина**	ЛКГ	$x_{i+1} = (105x_i \oplus 27) \bmod 2^8$, $x_0 = 52$, построить двоичную выходную последовательность (элементы мн-ва Z_{2^8} представлять в виде элементов мн-ва V_8)	Random Excursions Variant Test
32	**Мальцева**	(d,t)- шагов	$d=3, t=2,$ характеристический мн-н ЛРС-1 длины 18: (7,18), характеристический мн-н ЛРС-2 длины 16: (2,3,5,16), фильтрующая ф-ция: $f = x_{10} \oplus x_{12}x_{16} \oplus 1$	Test for the Longest Run of Ones in a Block
33	**Мельников**	A5/1	-	Frequency Test within a Block
34	**Музыченко**	Фильтрующий	ЛРС длины 27, характеристический мн-н: (1,2,5,27), фильтрующая ф-ция: $f = x_4x_{10} \oplus x_{18} \oplus 1$	Runs Test
35	**Окороков**	Комбинирующий	m=3, характеристический мн-н ЛРС-1 длины 26: (1,2,6,26), характеристический мн-н ЛРС-2 длины 25: (3,25), характеристический мн-н ЛРС-3 длины 23: (5,23), комбинирующая ф-ция: $f = x_1x_3 \oplus x_1x_2 \oplus x_2x_3$	Binary Matrix Run Test
36	**Подтуркин**	Геффе	Характеристический мн-н ЛРС-1 длины 21: (2,21), характеристический мн-н ЛРС-2 длины 20: (3,20), характеристический мн-н ЛРС- 3 длины 19: (1,2,5,19)	Discrete Fourier Transform (Spectral) Test
37	**Седова**	Пороговый	m=3, характеристический мн-н ЛРС-1 длины 16: (2,3,5,16), характеристический мн-н ЛРС-2 длины 15: (1,15), характеристический мн-н ЛРС- 3 длины 13: (1,3,4,13)	Non-overlapping Template Matching Test
38	**Скрипко**	$(\delta,\tau)-$ самоусечения	$\delta = 3, \tau = 2,$ характеристический мн-н ЛРС длины 32: (1,2,22,32), знак управляющей гаммы снимается с i-й ячейки регистра, i=11	Random Excursions Variant Test
39	**Соколов**	Сжимающий	Характеристический мн-н ЛРС-1 длины 12: (1,4,8,12), характеристический мн-н ЛРС-2 длины 11: (2,11)	Test for the Longest Run of Ones in a Block
40	**Филиппова**	С перемежающимся шагом	Характеристический мн-н ЛРС-1 длины 22: (1,22), характеристический мн-н ЛРС-2 длины 21: (2,21), характеристический мн-н ЛРС- 3 длины 20: (3,20), фильтрующая ф-ция: $f = x_{15}x_{16}x_{17} \oplus x_{19} \oplus 1$	Frequency Test within a Block
41	**Шмелев**	Стоп-вперед	Характеристический мн-н ЛРС-1 длины 27: (1,2,5,27), характеристический мн-н ЛРС-2 длины 21: (2,21), фильтрующая ф-ция: $f = x_3 \oplus x_{14}x_{15}$	Runs Test