1. Схема генератора.

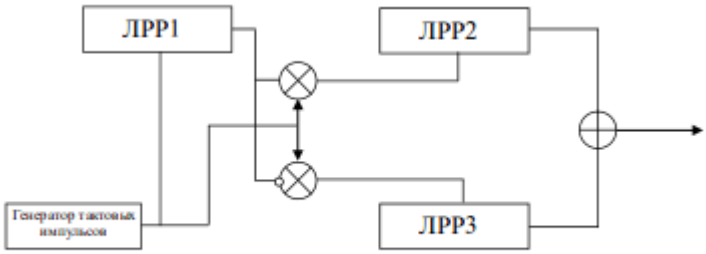


Рис.1. Схема генератора «стоп-пошёл»

2.Составим модели трех ЛРР в соответствии с выданным заданием. Зададим для них любые ненулевые начальные значения. Также сформируем итоговую ПСП.

На приведенных ниже рисунках изображены итоговые частотные характеристики (максимальные).

					Стат.характеристики				
					частота:	0,58	0,29	0,14	0,14	0,00
					число:	58	29	14	14	0
Начальное состояние	0	0	1	ПСП1	100	дл1	дл11	дл00	дл111	дл000
шаг 1	1	0	0	0		0				
шаг 2	1	1	0	0		0	0	1		
шаг 3	1	1	1	1		1	0	0	0	0
шаг 4	0	1	1	1		1	1	0	0	0
шаг 5	1	0	1	1		1	1	0	1	0
шаг 6	0	1	0	0		0	0	0	0	0
шаг 7	0	0	1	1		1	0	0	0	0

					Стат.характеристики				
					частота:	0,55	0,28	0,18	0,14	0,06
					число:	55	28	18	14	6
1	0	0	1	ПСП1	100	дл1	дл11	дл00	дл111	дл000
1	1	0	0	0		0				
0	1	1	0	0		0	0	1		
1	0	1	1	1		1	0	0	0	0
0	1	0	1	1		1	1	0	0	0

							Стат.характеристики				
							частота:	0,53	0,27	0,27	0,13	0,09
							число:	53	27	27	13	9
1	0	1	0	1	ПСП1		100	дл1	дл11	дл00	дл111	дл000
1	1	0	1	0	0			0				
1	1	1	0	1	1			1	0	0		
0	1	1	1	0	0			0	0	0	0	0
1	0	1	1	1	1			1	0	0	0	0

		Стат.характеристики				
	частота:	0,50	0,23	0,23	0,12	0,08
	число:	50	23	23	12	8
ИПСП	100	дл1	дл11	дл00	дл111	дл000
1		1				
1		1	1	0		
0		0	0	0	0	0
0		0	0	1	0	0
0		0	0	1	0	1
0		0	0	1	0	1
1		1	0	0	0	0
1		1	1	0	0	0
0		0	0	0	0	0
1		1	0	0	0	0
1		1	1	0	0	0

2. Проследим за поведением статистических характеристик в зависимости от изменения периода тестирования ПСП(100-200).

					Стат.характеристики				
				частота:	0,57	0,29	0,14	0,14	0,00
				число:	114	57	28	28	0
0	0	1	ПСП1	200	дл1	дл11	дл00	дл111	дл000
1	0	0	0		0				
1	1	0	0		0	0	1		
1	1	1	1		1	0	0	0	0
0	1	1	1		1	1	0	0	0
1	0	1	1		1	1	0	1	0

B	C	D	E	F	G	H	I	J	K	L
						Стат.характеристики				
					частота:	0,53	0,27	0,20	0,13	0,07
					число:	106	53	39	26	13
1	0	0	1	ПСП1	200	дл1	дл11	дл00	дл111	дл000
1	1	0	0	0		0				
0	1	1	0	0		0	0	1		
1	0	1	1	1		1	0	0	0	0

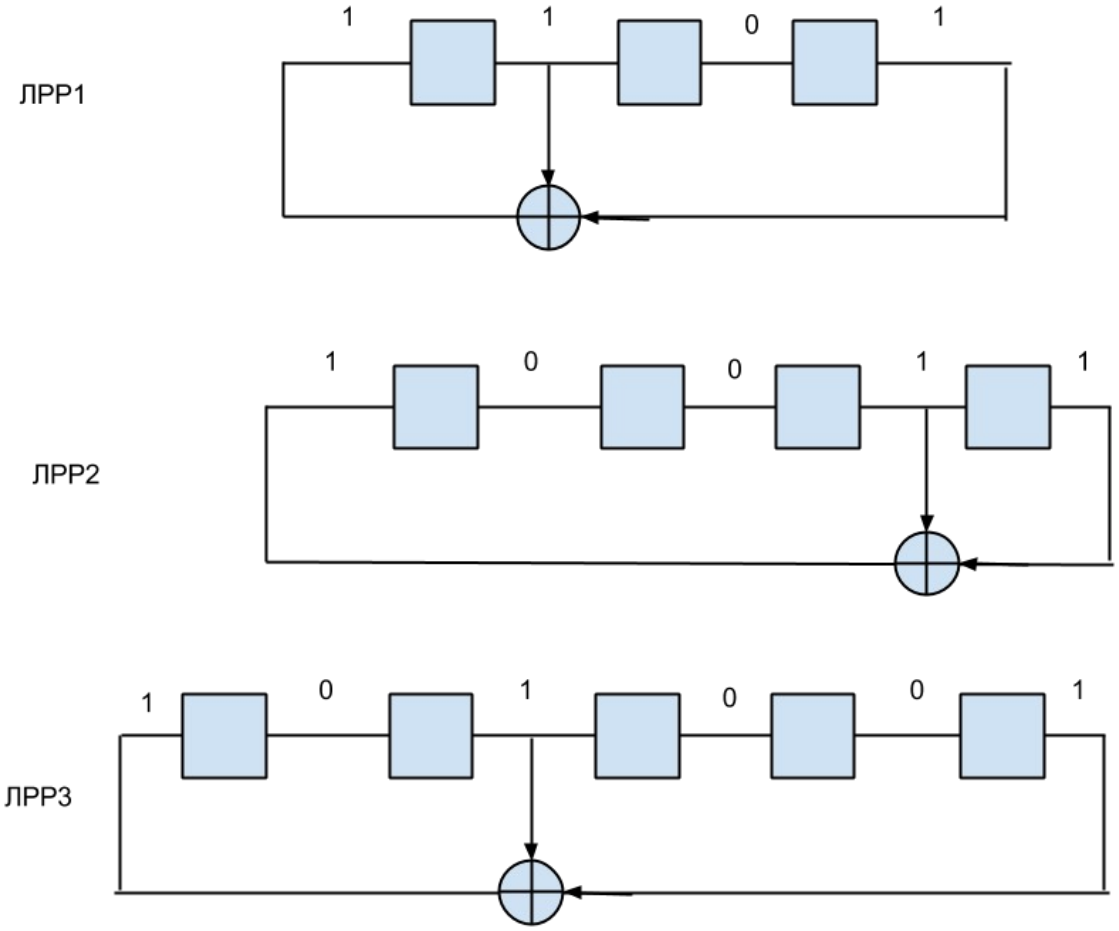
3.

	Стат.характеристики				
частота:	0,52	0,14	0,14	0,13	0,10
число:	103	27	27	25	19
200	дл1	дл11	дл00	дл111	дл000
	0				
	1	0	0		
	0	0	0	0	0
	1	0	0	0	0

4. Составим открытое сообщение в ASCII кодировке из 9 символов (из своего варианта), в котором один из символов повторяется трижды. Рассчитаем стохастические характеристики данной криптограммы. Ниже приведены таблица с исходными, зашифрованными, расшифрованными символами.

Исходный	Зашифр.	Расшифр.
О	CR**	О
П	i	П
Р	x	Р
С	ц	С
О	т	О
Т	™	Т
У	W	У
Ф	:	Ф
О	[	О

4. Составим схемотехнические модели ЛРР.



4. Составим математические модели ЛРР.

x^3+x^2+0*x+1=y

x^4+0*x^3+0*x^2+x+1=y

x^5+0*x^4+1*x3+0*x^2 + 0*x^1+1=y

Вывод: в ходе выполнения данной лабораторной работы были изучены особенности формирования псевдослучайных последовательностей для использования потоковых шифрах. Убедились, что даже одинаковые символы кодируются по-разному, что дает большую криптоустойчивости по сравнению с шифром простой замены.

Министерство образования и науки Российской Федерации
ФГОБУ ВПО «Санкт-Петербургский государственный университет
телекоммуникации им. проф. М.А. Бонч-Бруевича»
Кафедра безопасности информационных систем

ОТЧЁТ

по лабораторной работе №3 на тему:

«Исследование генераторов псевдослучайных последовательностей»

по дисциплине «Информационная безопасность и защита информации»

Выполнил: студент группы ИСТ 02, Приходько В.И.
Принял: к.п.н., доцент Ильяшенко О.Ю.

Санкт-Петербург
2014