МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «СГУ ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»

ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ

ЛАБОРАТОРНАЯ РАБОТА

студента 4 курса 431 группы
специальности 100501 — Компьютерная безопасность
факультета КНиИТ
Ивнановой Ксении

Проверил
доцент _____ И. И. Слеповичев

Саратов 2024

1 Параметры и результаты запуска программы

Линейный конгруэнтный метод

Параметры генерации:

python3 main.py -g lc -i 1024,1664525,1013904223,1 -n 10000 -f lc.dat

Аддитивный метод

Параметры генерации:

python3 main.py -g add -i 30000,24,55,79,134,213,347,560,907,1467,2374, 3841,6215,10056,16271,26327,12598,8925,21523,448,21971,22419,14390,6809, 21199,28 8520,18383,26903,15286,12189,27475,9664,7139,16803,23942,10745,4687,15432, 20119,5551,25670,1221,26891,28112,23779,17506 -n 10000 -f add.dat

Пятипараметрический метод

Параметры генерации:

python3 main.py -g 5p -i 89,7,13,24,10,234122131 -n 10000 -f 5p.dat

Регистр сдвига с обратной связью (РСЛОС)

Параметры генерации:

python3 main.py -g lfsr -i 10011011010011010,000101000111 -n 10000 -f lfsr.dat

Нелинейная комбинация РСЛОС

Параметры генерации:

python3 main.py -g nfsr -i 000000010101010,01011100000111101, 010101001100000,0001001,10000010010,000000001,1001 -f nfsr.dat -n 10000

Вихрь Мерсенна

Параметры генерации:

python3 main.py -g mt -i 1000,1234 -n 10000 -f mt.dat **RC4**

Параметры генерации:

python3 task1.py -g rc4 -i 213,968,838,64,355,214,212,36,695,139,897518,656, 956,810,510,985,105,670,8,907,951,685,989,222,931,169,286,289,556,731,902, 688,701,771,533,990,630,708,884,255,683,25,214,792,348,34,758,9,781,946, 580,615,955,585,5,886,563,81,38,809,444,619,222,544,53,635,621,630,251,497, 257,2,467,897,790,728,676,722,838,465,781,10,828,903,235,857,841,146,719,

681,678,961,652,491,38,256,909,251,21,110,811,273,25,642,286,489,478,184,812,
770,846,241,141,266,500,375,827,633,761,154,663,461,206,529,212,667,342,360,
165,523,749,582,803,553,345,786,990,361,702,256,380,234,238,73,965,266,300,
847,755,969,681,146,843,125,306,845,752,879,458,788,833,727,817,122,239,765,
877,827,327,733,658,644,880,150,474,493,689,670,368,611,263,113,417,834,103,
725,754,117,824,623,338,540,337,879,521,183,370,808,120,571,871,301,210,796,
744,398,106,845,745,842,876,399,27,105,601,802,831,53,266,157,352,175,303,
505,484,994,425,292,729,654,584,860,420,412,49,281,417,703,400,48,404,772,
389, 733,152,271,585,404,333,381,696,928,609,659,180,10 -f rc.dat -n 10000

ГПСЧ на основе RSA

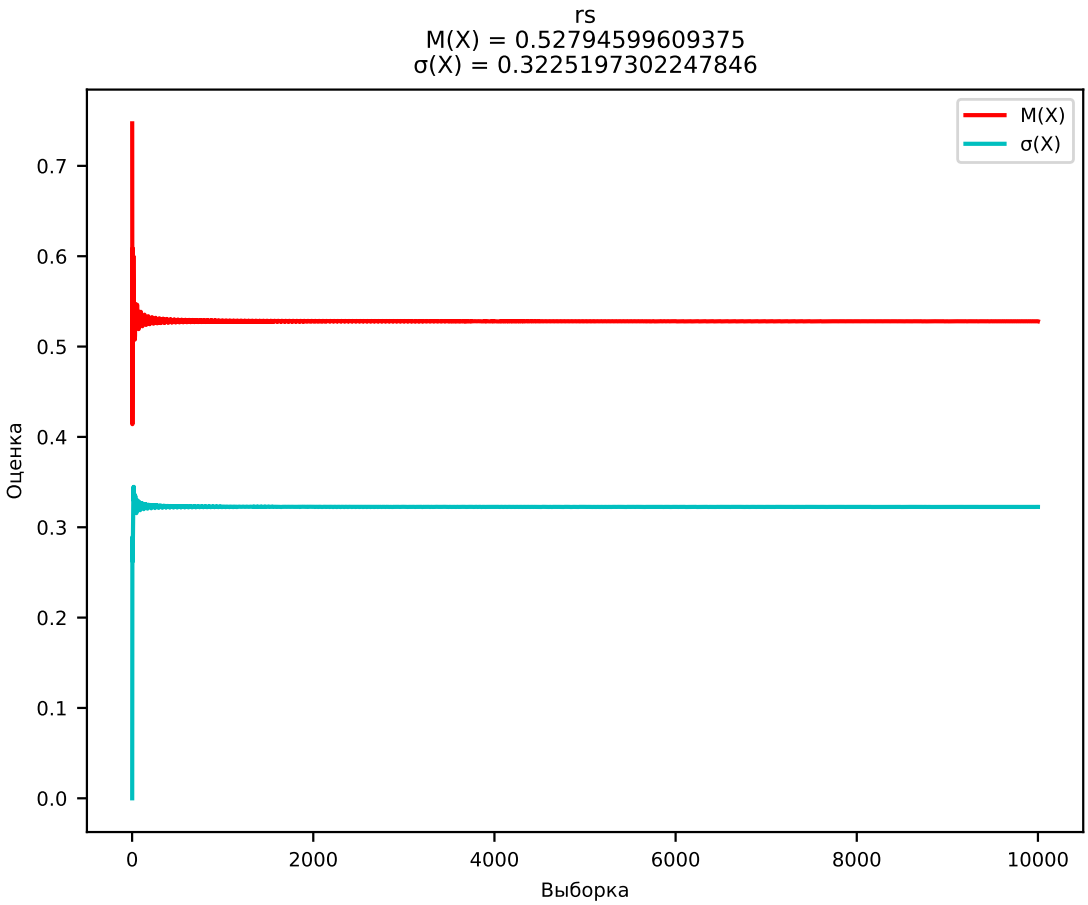
Параметры генерации:

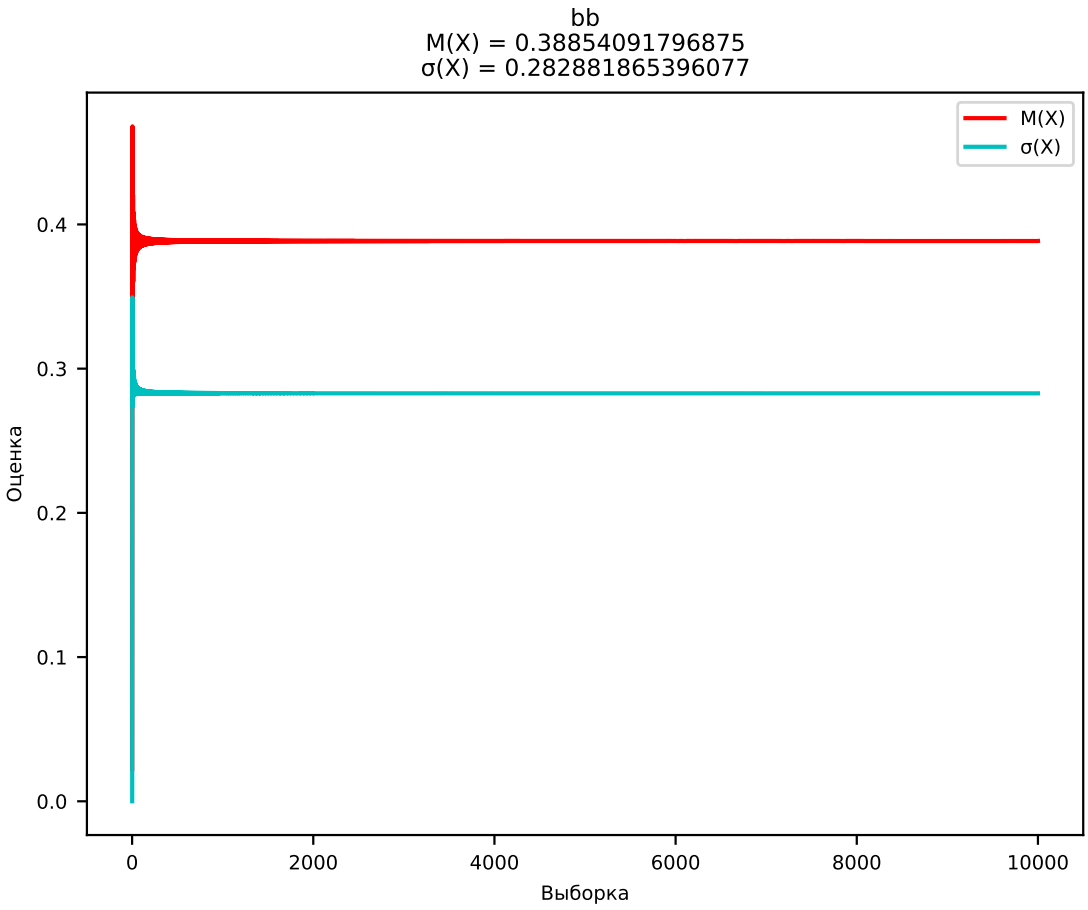
python3 main.py -g rsa -i 10967,571,77,10 -n 10000 -f rsa.dat

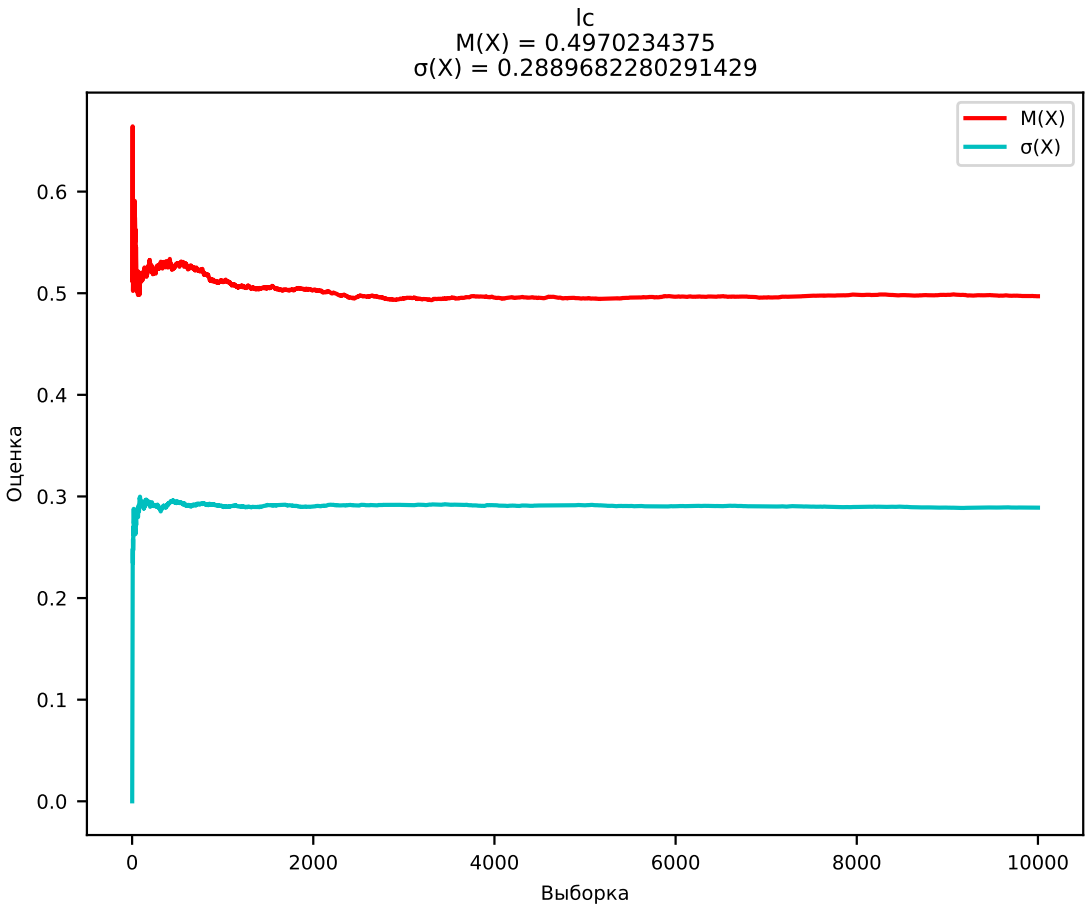
Алгоритм Блюм-Блюма-Шуба

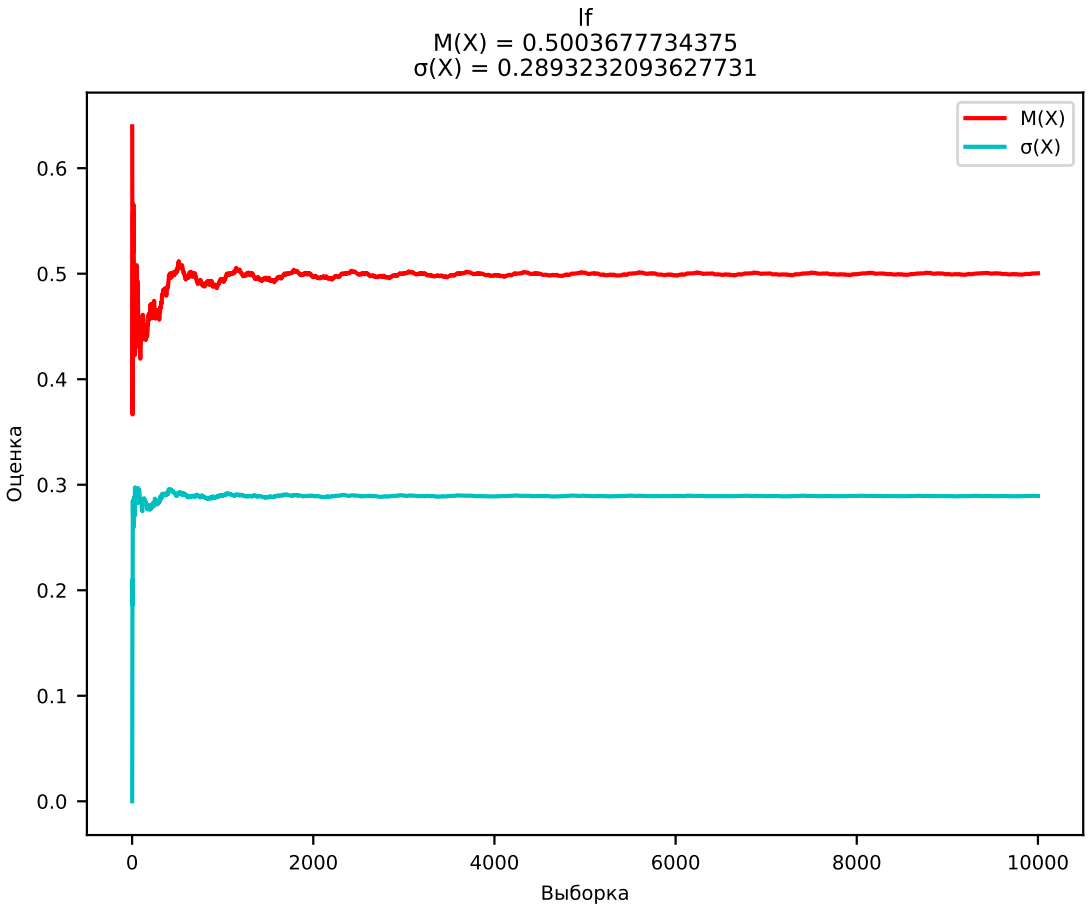
Параметры генерации:

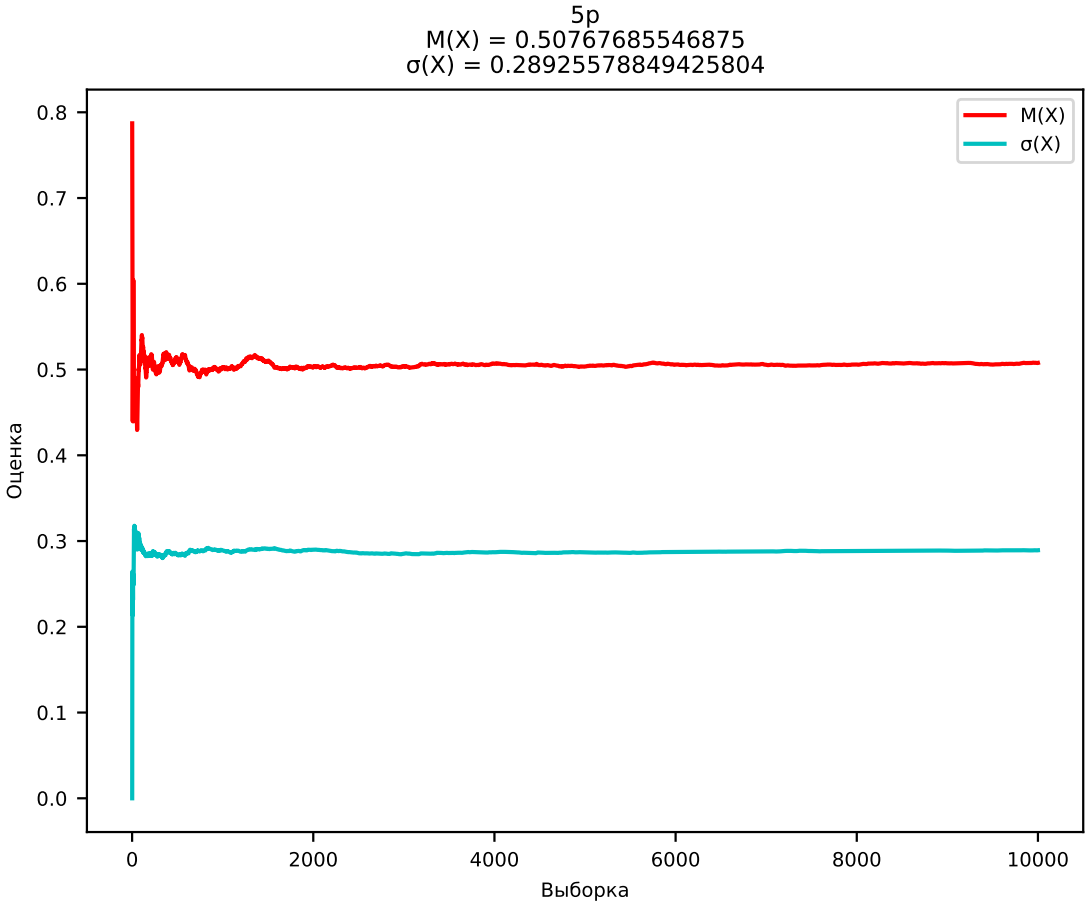
python3 main.py -g bbs -i 15621,10 -n 10000 -f bbs.dat

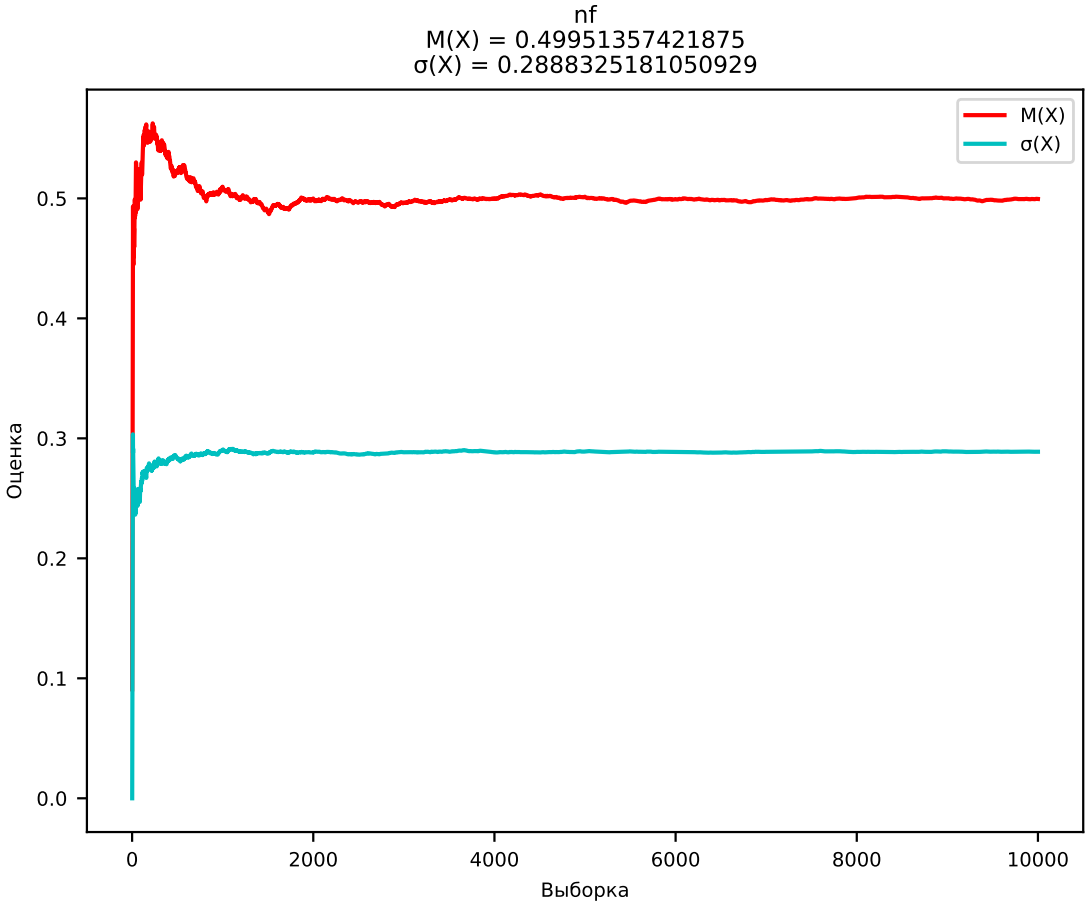

rs
M(X) = 0.52794599609375
σ(X) = 0.3225197302247846
M(X)
σ(X)
Оценка
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0
2000
4000
6000
8000
10000
Выборка


bb
M(X) = 0.38854091796875
σ(X) = 0.282881865396077
M(X)
σ(X)
0.4
0.3
0.2
0.1
0.0
Оценка
0
2000
4000
6000
8000
10000
Выборка


Ic
M(X) = 0.4970234375
σ(X) = 0.2889682280291429
M(X)
σ(X)
0.6
0.5
0.4
0.3
0.2
0.1
0.0
Оценка
0
2000
4000
6000
8000
10000
Выборка


lf
M(X) = 0.5003677734375
σ(X) = 0.2893232093627731
M(X)
σ(X)
0.6
0.5
0.4
0.3
0.2
0.1
0.0
Оценка
0
2000
4000
6000
8000
10000
Выборка


5p
M(X) = 0.50767685546875
σ(X) = 0.28925578849425804
M(X)
σ(X)
Оценка
Выборка
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0
2000
4000
6000
8000
10000


nf
M(X) = 0.49951357421875
σ(X) = 0.2888325181050929
M(X)
σ(X)
0.5
0.4
0.3
0.2
0.1
0.0
Оценка
0
2000
4000
6000
8000
10000
Выборка

1.1 Оценки параметров ППСЧ

	$M(X)$	$\sigma(X)$
lc	0.5001070313	0.2885282436
add	0.4959591797	0.2872104607
5p	0.5076768555	0.2892557885
lfsr	0.5003677734	0.2893232094
nfsr	0.4995135742	0.2888325181
mt	0.488571875	0.2811702731
rc4	0.4899671875	0.2894136027
rsa	0.5279459961	0.3225197302
bbs	0.388540918	0.2828818654

1.2 Проверка последовательностей на тестах

	lc	add	5p	lfsr	nfsr	mt	rc4	rsa	bbs
Хи-квадрат	+	+	+	+	-	-	-	-	-
серий	-	+	-	-	-	-	-	-	+
интервалов	+	-	+	+	+	+	+	+	-
разбиений	-	+	-	-	-	-	-	-	-
перестановок	-	+	-	-	-	-	-	-	-
монотонности	-	+	-	-	-	-	-	-	-