

**Частное акционерное общество
«Институт информационных технологий»**

**Инструкция по использованию программного
обеспечения Generation_Sboxes для генерации
нелинейных таблиц замены симметричного
блочного шифра «Калина» ДСТУ 7624:2014**

Харьков 2015

1. Функциональное назначение и структура

Программное обеспечение (ПО) `Generation_Sboxes` предназначено для генерации нелинейных таблиц замены (S-блоков) блочного симметричного шифра «Калина» (может использоваться и для других криптографических примитивов). ПО предусматривает генерацию S-блоков на основе различных векторных булевых функций и с различной нелинейностью.

Структурная схема ПО приведена на рис.1. Файл параметров конфигурации `parameters.txt` поступает на вход программы `Generation_Sboxes`. Для генерации нелинейных таблиц замены программа использует файл со случайными данными (источник энтропии). Результатом работы программы являются сгенерированные S-блоки, которые вместе с их характеристиками записываются в файл `S-boxes.txt`.



Рис. 1. Структурная схема ПО

2. Технические средства

ПО может использоваться на персональном компьютере с операционными системами Windows, Linux. Для каждой ОС предоставляется свой исполняемый файл `Generation_Sboxes`.

3. Вызов и загрузка

Для того чтобы выполнить генерацию S-блоков необходимо выполнить следующие шаги.

1. В директорию с файлом `Generation_Sboxes` поместить файл со случайными данными (источник энтропии) с расширением `.dat`.

Требование к файлу со случайными данными: файл должен содержать случайную последовательность байт, соответствующую равномерному закону распределения с независимыми значениями случайной величины (желательно, получить такую

последовательность от криптографического аппаратного датчика случайных последовательностей).

Для генерации одного S-блока необходим следующий размер случайных данных:

- при значении параметра `non_linearity` = 100, 102 не менее 10 Кб;
- при значении параметра `non_linearity` = 104 не менее 80 Мб.

2. Задать значения параметров конфигурации в соответствии с п. 3.

3. Из командной строки запустить файл `Generation_Sboxes`.

4. Входные данные

Входные данные для работы программы задаются пользователем в файле параметров конфигурации `parameters.txt`.

Пример файла параметров конфигурации `parameters.txt` приведен в приложении А.

В файле `parameters.txt` необходимо задать значения параметров, представленных в табл. 1.

Таблица 1

Имя параметра	Описание параметра	Допустимые значения
<code>initial_pow</code>	Вид степенной функции (фиксируемый или случайно выбираемый)	127, 191, 223, 239, 247, 251, 253, 254, random
<code>number_Sboxes</code>	Количество S-блоков, которое необходимо сгенерировать	≥ 1
<code>non_linearity</code>	Значение нелинейности (с увеличением значения повышается запас стойкости)	100, 102, 104
<code>random_data</code>	Путь к файлу со случайными данными	Файл должен иметь расширение <code>.dat</code>

После имени параметра и знака «=» необходимо ввести значение данного параметра. Допустимые значения всех параметров представлены в файле `parameters.txt` в виде комментариев.

Отсутствие хотя бы одного из параметров или некорректное его значение приводит к ошибке и преждевременному завершению работы программы. Подробная информация о возможных ошибках изложена в п. 5.

5. Выходные данные

Выходными данными работы программы являются сгенерированные S-блоки. В результате работы программы создается файл S-boxes.txt, в который записываются характеристики сгенерированных S-блоков, сами S-блоки и время, затраченное на их генерацию.

При каждом новом запуске программы предыдущее содержимое файла S-boxes.txt удаляется.

Примеры сформированных S-блоков приведены в приложении Б.

6. Обработка ошибок

В табл. 2 приведен список ошибок, которые могут возникнуть в процессе работы программы.

Таблица 2

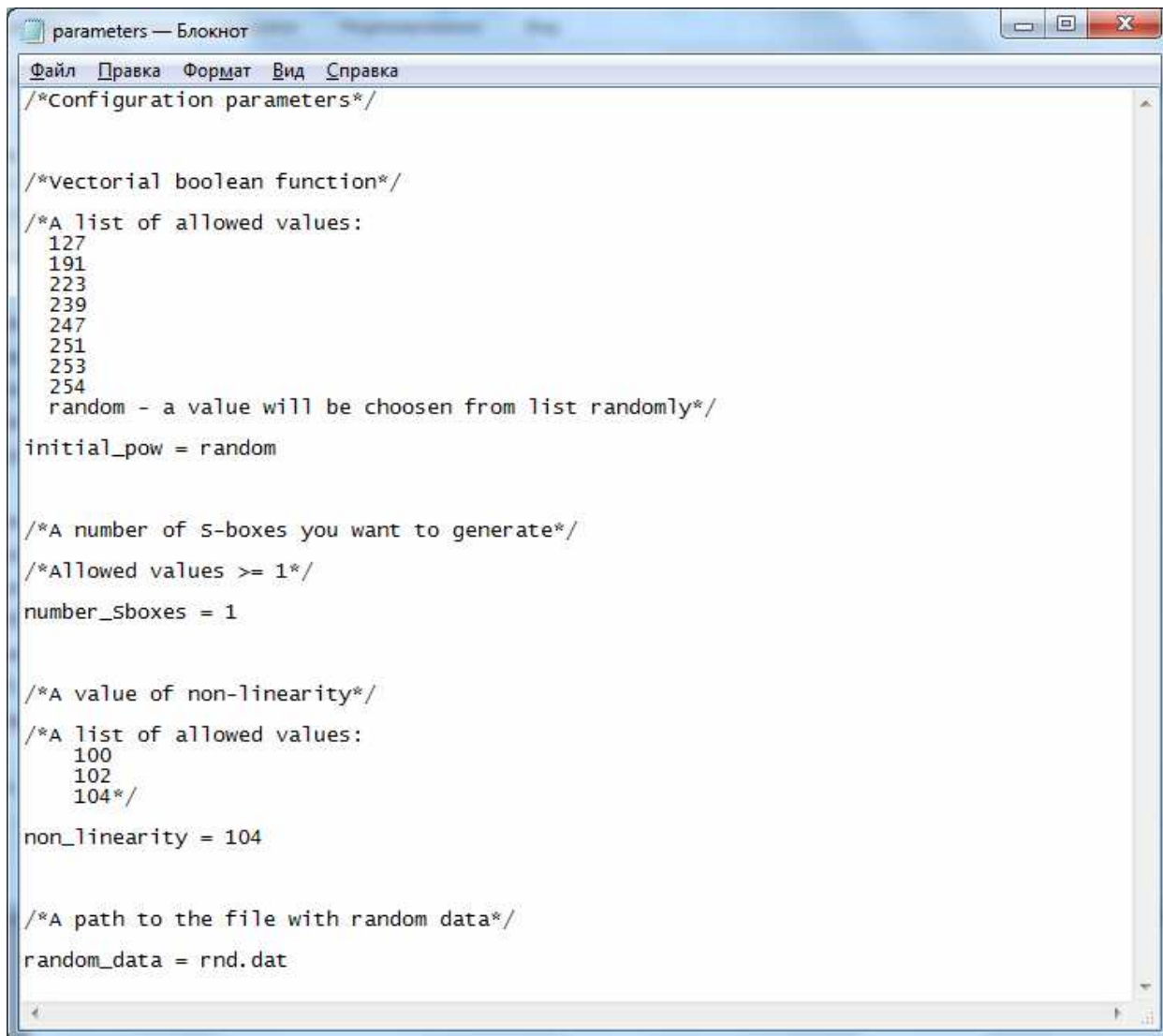
Сообщение об ошибке	Причина ошибки
Can't open file parameters.txt! Check that file parameters.txt exists and it is in the same folder than Generation_Sboxes.exe.	Файл параметров конфигурации parameters.txt отсутствует в папке с исполняемым файлом.
The value of initial_pow is incorrect! Please, check it in parameters.txt	Значение параметра initial_pow некорректно. Необходимо удостовериться, что введенное значение входит в список допустимых значений, прописанный в файле parameters.txt.
The value of number_Sboxes is incorrect! Please, check it in parameters.txt	Значение параметра number_Sboxes некорректно. Необходимо удостовериться, что введенное значение входит в список допустимых значений, прописанный в файле parameters.txt.
The value of non_linearity is incorrect! Please, check it in parameters.txt	Значение параметра non_linearity некорректно. Необходимо удостовериться, что введенное значение входит в список допустимых значений, прописанный в файле parameters.txt.
Can't open file "имя_файла"! Check value of random_data in parameters.txt	Невозможно открыть файл со случайными данными. Возможно, имя файла задано некорректно в файле parameters.txt.
File "имя_файла" is empty! Please, check value of random_data in parameters.txt	Файл со случайными данными пуст.
File parameters.txt was corrupted! There no 'initial_pow' parameter.	Нарушена целостность файла parameters.txt: отсутствует параметр initial_pow.
File parameters.txt was corrupted! There no 'number_Sboxes' parameter.	Нарушена целостность файла parameters.txt: отсутствует параметр number_Sboxes.

Таблица 2 (продолжение)

Сообщение об ошибке	Причина ошибки
File parameters.txt was corrupted! There no 'non_linearity' parameter.	Нарушена целостность файла parameters.txt: отсутствует параметр non-linearity.
File parameters.txt was corrupted! There no 'random_data' parameter.	Нарушена целостность файла parameters.txt: отсутствует параметр random_data.
Warning: the end of file with random data!	Достигнут конец файла со случайными данными.
Generation has been interrupted. "количество_сгенерированных_S-блоков" S-boxes are in S-boxes.txt	Генерация подстановок преждевременно завершена в виду достижения конца файла со случайными данными.

Приложение А

Пример файла параметров конфигурации parameters.txt



```
parameters — Блокнот
Файл Правка Формат Вид Справка
/*Configuration parameters*/

/*vectorial boolean function*/
/*A list of allowed values:
127
191
223
239
247
251
253
254
random - a value will be choosen from list randomly*/
initial_pow = random

/*A number of s-boxes you want to generate*/
/*Allowed values >= 1*/
number_sboxes = 1

/*A value of non-linearity*/
/*A list of allowed values:
100
102
104*/
non_linearity = 104

/*A path to the file with random data*/
random_data = rnd.dat
```

Приложение Б

Пример сформированного S-блока

В табл. 1 в десятичном представлении приведен пример сформированного S-блока на основе степенной векторной булевой функции x^{254} со следующими характеристиками:

- нелинейность 104;
- максимум таблицы дифференциалов 8;
- максимум таблицы линейных аппроксимаций 24;
- минимальная степень S-блока 7;
- алгебраический иммунитет 3;
- циклическая структура: 0:205, 10:47, 143:4 (где первое число – первый элемент цикла, второе – длина цикла).

Таблица 1

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	26	168	150	161	166	151	128	38	193	242	50	127	139	201	240	195
1	100	121	39	16	67	76	108	155	196	172	216	234	178	158	213	142
2	125	2	199	14	23	131	203	7	97	224	132	250	62	3	122	36
3	190	140	25	111	29	247	184	104	179	230	120	219	209	205	10	167
4	163	180	241	252	63	93	87	79	66	141	202	113	95	171	102	217
5	160	114	22	173	156	44	73	48	187	153	49	206	52	60	254	211
6	24	208	239	207	130	54	204	109	214	183	198	92	88	134	32	228
7	117	126	135	65	138	83	31	33	99	103	116	55	12	45	145	72
8	84	223	56	115	68	177	174	64	42	98	251	197	245	28	77	175
9	69	112	220	149	4	236	15	188	253	107	13	162	46	147	58	235
a	89	170	192	85	6	237	225	80	75	215	90	101	74	227	37	169
b	200	181	91	118	71	5	20	34	47	129	154	11	194	119	9	53
c	144	30	233	61	123	244	81	146	41	51	176	157	35	210	18	106
d	137	43	212	40	221	246	248	143	8	105	57	0	165	229	226	136
e	82	27	249	218	191	185	243	96	19	255	86	124	222	110	94	133
f	59	159	232	17	78	189	148	164	70	186	238	21	152	1	182	231