ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Факультет компьютерных наук
Департамент программной инженерии

СОГЛАСОВАНО
Зам. директора по работе с НИУ
ООО «1С»

_____ Н.Ю. Старичков
«12» мая 2022г.

УТВЕРЖДАЮ
Академический руководитель
образовательной программы
«Программная инженерия»
профессор департамента
программной инженерии,
канд. техн. наук

_____ В.В. Шилов
«12» мая 2022 г.

КРИПТОГРАФИЧЕСКИ СТОЙКИЙ
ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Руководство оператора

ЛИСТ УТВЕРЖДЕНИЯ

RU.17701729.03.10-01 34 01-1-ЛУ

Исполнитель:
студент группы БПИ201
_____ / Камнев П.А. /
«12» мая 2022 г.

Москва 2022

Инв. № подл	RU.17701729.03.10-01 34 01-1-ЛУ
Подп. и дата	
Взам. инв. №	
Инв. № дубл.	
Подп. и дата	

УТВЕРЖДЕН
RU.17701729.03.10-01 34 01-1-ЛУ

КРИПТОГРАФИЧЕСКИ СТОЙКИЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Руководство оператора

RU.17701729.03.10-01 34 01-1

Листов 8

Инв. № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата
RU.17701729.03.10-01 34 01-1				

Москва 2022

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Функциональным назначением разрабатываемой программы является генерация псевдослучайных последовательностей натуральных чисел с возможностью указания количества и диапазона генерируемых чисел, а также генерация псевдослучайных последовательностей бит.

Программа может быть использована в любых целях, которые требуют генерации равномерно распределенных псевдослучайных последовательностей чисел или псевдослучайных последовательностей бит, в частности, в криптографических целях: для генерации ключей шифрования, для генерации случайных паролей, для генерации токенов доступа. Таким образом, программа позволяет генерировать псевдослучайные последовательности для таких целей, в которой является критической возможность предсказания следующих элементов псевдослучайной последовательности на основе предыдущих

Функции программы:

1. Программа позволяет генерировать последовательности равномерно распределенных псевдослучайных чисел.
   1.1. Возможно задать промежуток, на котором будут равномерно распределены генерируемые числа.
   1.2. Программа позволяет генерировать числа в промежутке от 0 до 2^{32} - 1.
2. Программа позволяет генерировать псевдослучайные последовательности бит.
3. Программа позволяет инициализировать псевдослучайный генератор как от энтропии устройства, так и от целых чисел от 0 до 2^{32} - 1 (в таком случае каждый раз генерируется одинаковая последовательность).
4. Программа позволяет выводить генерируемую последовательность как в консоль, так и в файл.
5. Присутствует режим тестирования, позволяющий непрерывно выводить генерируемую последовательность до внешнего завершения процесса.
6. Программа запускается через консоль и позволяет задавать через аргументы командной строки параметры генерации псевдослучайных последовательностей.
   6.1. Тип генерируемых значений – числа или биты.
   6.2. При генерации чисел – промежуток, по которому будут равномерно распределены генерируемые числа.
   6.3. Длина генерируемой последовательности. Для генерации чисел – количество чисел, которые будут сгенерированы. Для генерации последовательностей бит – длина псевдослучайной последовательности в байтах.
   6.4. Формат выходных данных – вывод последовательности в консоль или в файл.
   6.5. Имя выходного файла (в случае генерации последовательности в файл).
   6.6. Инициализация псевдослучайного генератора некоторым числом или случайной энтропией, полученной от устройства, на котором происходит запуск.
   6.7. Также присутствует опция тестирования, при наличии которой генератор будет непрерывно выводить последовательность бит в консоль до внешнего завершения процесса.
7. В случае ввода некорректных параметров через аргументы командной строки в консоль выводится информация о том, в каком виде задаются параметры, программа завершает свое выполнение.
8. При генерации значений в файл программа проверяет доступное место на диске. Если места на диске недостаточно, в консоль выводится ошибка, программа завершает свое выполнение.
9. При возникновении ошибок, связанных с получением энтропии от устройства, в консоль выводится краткая информация об ошибке, программа завершает свое выполнение.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Требования к составу и параметрам технических средств

Рекомендуемые минимальные параметры устройства для стабильного функционирования программы:

- Pentium-совместимый процессор с частотой 233 MHz;
- 64 МБ оперативной памяти;
- 1,5 ГБ свободного места на диске;
- клавиатура;
- видеоадаптер и монитор с разрешением Super VGA (800 x 600).

Минимальные требования к ПО для стабильного функционирования программы:

- операционная система Windows (версии XP и старше).

2.2. Требования к квалификации оператора

Пользователь программы должен обладать базовыми навыками работы с персональным компьютером, а также с консольными приложениями.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Консольная утилита

3.1.1. Запуск программы

Для базового запуска утилиты достаточно запустить исполняемый файл через командную строку.

```
\SecureGenerator\x64\Release>secure-generator.exe
709543613
```

Рисунок 1. Запуск утилиты генерации в режиме командной строки

3.1.2. Использование опций программы

Запуск генератора через командную строку происходит следующим образом:
secure-generator.exe [опции] <параметры>

3.1.2.1. Генерация бит

Используя опцию --bits, можно генерировать последовательности псевдослучайных бит. Открыть бинарный файл можно при помощи Hex Editor Neo.

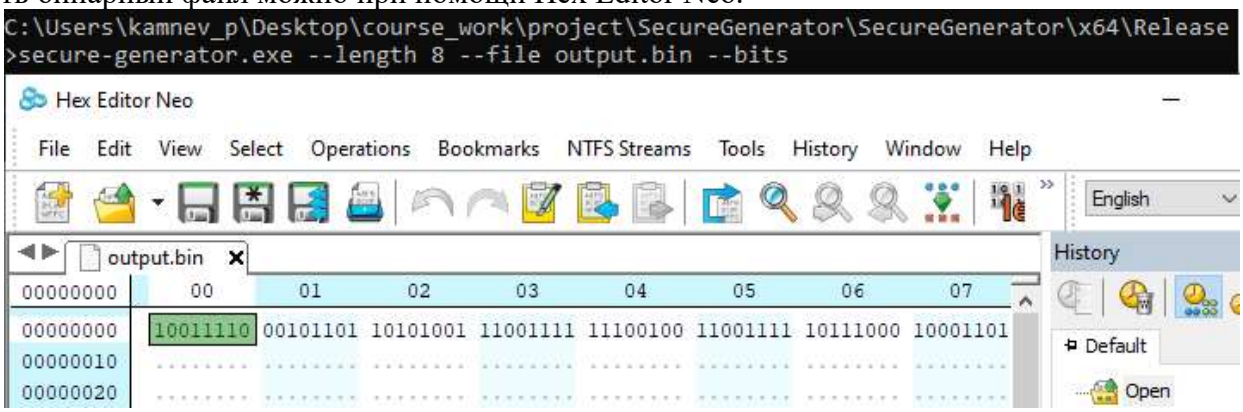

Рисунок 2. Генерация битовых псевдослучайных данных

3.1.2.2. Задание границ диапазона генерируемых чисел

Опции --min и --max позволяют задавать минимальное и максимальное значение генерируемых чисел. При их использовании числа должны находиться в заданном промежутке.

```
>secure-generator.exe --length 10 --min 1 --max 10
10 7 5 9 8 9 2 8 4 6
```

Рисунок 3. Генерация чисел в заданном промежутке

3.1.2.3. Задание длины генерируемой последовательности

С использованием опции --length <длина> можно задать длину генерируемой последовательности псевдослучайных чисел (в случае использования опции --bits задается количество генерируемых байт).

```
>secure-generator.exe --length 100
2609972078 2151823485 2424549219 2381842149 3220832706 1661562369 3479373954 1358672147 3
77383076 1346969959 2939121576 1396775224 2872492127 1877332067 1912451990 2612439091 210
5640083 1290383374 1576238054 3938097001 2376025305 2115967990 1194973326 2354700819 4148
761079 2403494448 4124774399 1008681904 517236767 1886474819 2207769736 3282987504 126859
3023 1041737572 2174484487 3568795693 4109167744 770025831 1866847648 2203073092 12912989
38 560808031 3261111859 1125977603 91829280 3576522354 2954684916 4171664657 1197490241 6
30728424 2174963408 1197863869 3136932048 787685766 2070620579 2072496878 939221369 40709
1787 2085427269 911703073 1424646182 3219990777 3844553198 3622112214 3292012428 34471948
63 1191387651 2153789548 772002401 1941331236 1562039448 514464906 3286513239 3733033054
3130109187 1358500646 3599054502 3400342726 3755408717 3144627027 1185905667 2881761591 1
370553882 3193408235 4024384646 278055139 3516537535 344727985 1633080596 584713893 41050
69385 389408844 704303901 3475890943 1511572980 1755106149 3349245099 3416819540 40781349
89 2027634020
```

Рисунок 4. Генерация последовательности из нескольких псевдослучайных чисел

3.1.2.4. Генерация в файл

При использовании опции --file <имя> в папке с исполняемым файлом должен появляться файл <имя>, содержащий сгенерированную последовательность

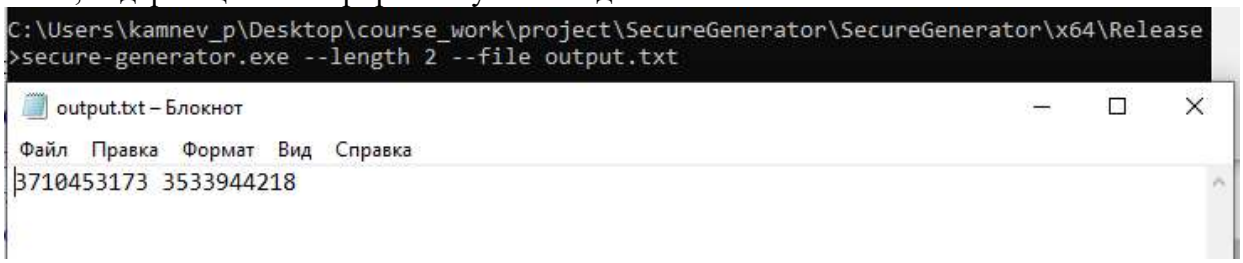

Рисунок 2. Генерация значений в файл

3.1.2.5.Инициализация генератора от энтропии устройства и от целого числа

При инициализации генератора без опции --seed происходит инициализация генератора от энтропии устройства – генерируемые последовательности каждый раз отличаются.

```
C:\Users\kamnev_p\Desktop\course_work\project\SecureGenerator\SecureGenerator\x64\Release
>secure-generator.exe --length 2
1799592510 2684262492
C:\Users\kamnev_p\Desktop\course_work\project\SecureGenerator\SecureGenerator\x64\Release
>secure-generator.exe --length 2
2040239678 777202320
```

Рисунок 6. Инициализация генератора энтропией устройства

Если использовать опцию --seed, при одинаковом значении параметра генератор каждый раз генерируете одну и ту же последовательность.

```
C:\Users\kamnev_p\Desktop\course_work\project\SecureGenerator\SecureGenerator\x64\Release
>secure-generator.exe --length 2 --seed 1
151440905 1449946105
C:\Users\kamnev_p\Desktop\course_work\project\SecureGenerator\SecureGenerator\x64\Release
>secure-generator.exe --length 2 --seed 1
151440905 1449946105
```

Рисунок 7. Инициализация генератора одним и тем же числом

3.1.2.6.Опция тестирования

При использовании опции --test_mode утилита выводит сырой поток бит в консоль. Генератор можно протестировать, например, при помощи тестовой утилиты PractRand.

```
C:\Users\kamnev_p\Desktop\course_work\project\SecureGenerator\SecureGenerator\Release>SecureGenerator.exe --test_mode |
 .\..\..\..\PractRand_094\bin\msvc12_64bit\RNG_test.exe stdin
RNG_test using PractRand version 0.94
RNG = RNG_stdin, seed = unknown
test set = core, folding = standard(unknown format)

rng=RNG_stdin, seed=unknown
length= 128 megabytes (2^27 bytes), time= 2.7 seconds
  no anomalies in 196 test result(s)

rng=RNG_stdin, seed=unknown
length= 256 megabytes (2^28 bytes), time= 5.8 seconds
  no anomalies in 213 test result(s)

rng=RNG_stdin, seed=unknown
length= 512 megabytes (2^29 bytes), time= 11.4 seconds
  no anomalies in 229 test result(s)

rng=RNG_stdin, seed=unknown
length= 1 gigabyte (2^30 bytes), time= 22.4 seconds
  no anomalies in 248 test result(s)

rng=RNG_stdin, seed=unknown
length= 2 gigabytes (2^31 bytes), time= 44.0 seconds
  no anomalies in 266 test result(s)
```

Рисунок 8. Режим тестирования

3.1.3. Возможные сообщения

В случае ввода некорректных параметров через аргументы командной строки в консоль выводится информация о том, в каком виде задаются параметры, программа завершает свое выполнение.

```
C:\Users\kamnev_p\Desktop\course_work\project\SecureGenerator\SecureGenerator\x64\Release>secure-generator.exe --distribution
Доступны следующие опции:
--bits (генерация бит, по умолчанию генерируются числа)
--min (нижняя граница промежутка генерируемых чисел), параметром является целое число в промежутке от 0 до 2^32 - 1, по умолчани
ю принимает значение 0
--max (верхняя граница промежутка генерируемых чисел), параметром является целое число в промежутке от 0 до 2^32 – 1;
--length (длина генерируемой последовательности, при генерации чисел – количество чисел, при генерации бит – количество байт), п
араметром является целое число не менее 1, по умолчанию принимает значение 1
--file (вывод в файл, по умолчанию вывод в консоль), параметром является имя файла со сгенерированными значениями, который будет
 создан в каталоге, где расположен исполняемый файл
--seed (инициализировать генератор числом, по умолчанию происходит инициализация энтропией устройства), параметром является цело
е число в промежутке от 0 до 2^32 - 1
--test_mode (режим тестирования), при выборе этой опции генерируются псевдослучайные биты и непрерывно выводятся в консоль до вн
ешнего завершения процесса, единственная доступная опция при наличии данного параметра – инициализация числом (--seed)
```

Рисунок 9. Неправильный параметр

При использовании несовместимых опций (--bits и --min или --max, --test_mode и любая другая опция, кроме --seed) выводится ошибка.

```
C:\Users\kamnev_p\Desktop\course_work\project\SecureGenerator\SecureGenerator\Release>SecureGenerator.exe --bits --min 2

Использованы несовместимые опции --bits и --min.
```

Рисунок 10. Использование несовместимых опций

Если указана опция, но не указан ее параметр (кроме --bits и –test_mode), выводится ошибка.

```
>SecureGenerator.exe --min
Не указан параметр для опции --min
```

Рисунок 11. Не указан параметр для опции

При генерации значений в файл программа проверяет доступное место на диске. Если места на диске недостаточно, в консоль выводится ошибка, программа завершает свое выполнение.

```
C:\Users\kamnev_p\Desktop\course_work\project\SecureGenerator\SecureGenerator\Release>SecureGenerator.exe
 --file out --length 1000000000000000
На диске недостаточно свободного места для генерации значений в файл. Проверьте параметр --length.
```

Рисунок 12. На диске недостаточно места для генерации значений в файл

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц в докум.)	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
Изм.	Измененных	Заменен ных	Новых	Аннулированных					

Изм.	Лист	№ докум.	Подп.	Дата
RU.17701729.03.10-01 34 01-1				
Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата