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

Техническое задание

ЛИСТ УТВЕРЖДЕНИЯ

RU.17701729.03.10-01 ТЗ 01-1-ЛУ

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

Москва 2022

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

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

КРИПТОГРАФИЧЕСКИ СТОЙКИЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Техническое задание

RU.17701729.03.10-01 ТЗ 01-1

Листов 18

Москва 2022

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

СОДЕРЖАНИЕ

АННОТАЦИЯ

Данное техническое задание на разработку «Криптографически стойкого генератора псевдослучайных чисел» содержит следующие разделы: «Введение», «Основание для разработки», «Назначение разработки», «Требования к программе», «Требования к программным документам», «Технико-экономические показатели», «Стадии и этапы разработки», «Порядок контроля и приемки» и приложения.

В разделе «Введение» указано наименование и краткая характеристика области применения программы.

В разделе «Основания для разработки» указан документ, на основании которого ведется разработка и наименование темы разработки.

В разделе «Назначение разработки» указано функциональное и эксплуатационное назначение программы.

В разделе «Требования к программе» указаны основные требования к функциональным характеристикам, к надежности, к условиям эксплуатации, к составу и параметрам технических средств, к информационной и программной совместимости, к маркировке и упаковке, к транспортировке и хранению, а также специальные требования.

В разделе «Требования к программным документам» указан предварительный состав программной документации и специальные требования к ней.

В разделе «Технико-экономические показатели» указаны ориентировочная экономическая эффективность, предполагаемая потребность, экономические преимущества разработки по сравнению с лучшими отечественными и зарубежными образцами или аналогами.

В разделе «Стадии и этапы разработки» установлены стадии разработки, этапы и содержание работ.

В разделе «Порядок контроля и приемки» указаны виды испытаний и общие требования к приемке работы.

Настоящий документ разработан в соответствии с требованиями:

1) ГОСТ 19.101-77 Виды программ и программных документов [1];
2) ГОСТ 19.102-77 Стадии разработки [2];
3) ГОСТ 19.103-77 Обозначения программ и программных документов [3];
4) ГОСТ 19.104-78 Основные надписи [4];
5) ГОСТ 19.105-78 Общие требования к программным документам [5];
6) ГОСТ 19.106-78 Требования к программным документам, выполненным печатным способом [6];
7) ГОСТ 19.404-79 Пояснительная записка. Требования к содержанию и оформлению [7].

1. ВВЕДЕНИЕ

Наименование: Криптографически стойкий генератор псевдослучайных чисел.

Наименование на английском языке: Cryptographically secure pseudorandom number generator.

Краткая характеристика и область назначения: Программа, генерирующая последовательности псевдослучайных чисел, которые можно использовать для криптографических целей (например, для генерации ключей).

2. ОСНОВАНИЯ ДЛЯ РАЗРАБОТКИ

Документ, на основании которого ведется разработка:

Основанием для разработки программы является Учебный план подготовки бакалавров по направлению 09.03.04 «Программная инженерия» и утвержденная академическим руководителем программы тема курсового проекта.

Название темы разработки на русском языке: Криптографически стойкий генератор псевдослучайных чисел.

Название темы разработки на английском языке: Cryptographically secure pseudorandom number generator.

3. НАЗНАЧЕНИЕ РАЗРАБОТКИ

3.1. Функциональное назначение

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

3.2. Эксплуатационное назначение

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.

4. ТРЕБОВАНИЯ К ПРОГРАММЕ

4.1. Требования к функциональным характеристикам

4.1.1. Требования к составу выполняемых функций

1. Программа должна позволять генерировать последовательности равномерно распределенных псевдослучайных чисел.
   1.1. Возможно задать промежуток, на котором будут равномерно распределены генерируемые числа.
   1.2. Программа должна позволять генерировать числа в промежутке от 0 до 2^{32} - 1.
2. Программа должна позволять генерировать псевдослучайные последовательности бит.
3. Программа должна позволять 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 должна позволять выводить генерируемую последовательность как в консоль, так и в файл.
5. Должен присутствовать режим тестирования, позволяющий непрерывно выводить генерируемую последовательность до внешнего завершения процесса.
6. Программа должна запускаться через консоль и позволять 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 должна присутствовать 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.

4.1.2. Требования к интерфейсу

Взаимодействие пользователя с программой происходит через интерфейс командной строки (консоль).
Запуск генератора через командную строку происходит следующим образом:

secure-generator.exe [опции] [параметры]

Должны быть 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 умолчанию принимает значение 0;
- --max (верхняя граница промежутка генерируемых чисел), параметром является целое число в промежутке от 0 до 2^{32} - 1, по умолчанию принимает значение 2^{32} - 1;
- --length (длина генерируемой последовательности, при генерации чисел – количество чисел, при генерации бит – количество байт), параметром 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 целое 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 внешнего завершения процесса, единственная доступная опция при наличии данного параметра – инициализация числом.

Пример (генерация 20 псевдослучайных чисел в промежутке от 1 до 10 в файл output.txt):

secure-generator.exe --min 1 --max 10 --length 20 --file output.txt

4.1.3. Требования к организации входных данных

Входными данными являются параметры работы программы, вводимые в виде аргументов командной строки.

4.1.4. Требования к организации выходных данных

В случае вывода генерируемых последовательностей в файл, создается файл с именем, заданным пользователем через аргументы командной строки. В противном случае генерируемые последовательности выводятся в консоль.
- При генерации последовательностей чисел генерируемые числа выводятся через пробел (без дополнительных выходных данных).
- При генерации последовательностей бит происходит вывод двоичных данных (сгенерированные файлы можно просмотреть при помощи специальных редакторов двоичных данных).

4.1.5. Требования к временным характеристикам

Временные характеристики зависят от характеристик устройства, на котором производится тестирования. На устройстве, на котором производится тестирование, время генерации 1 000 000 000 целых чисел в промежутке 0 до 2^{32} - 1 при помощи разрабатываемого генератора должно превышать не более чем в 10 раз время генерации 1 000 000 000 целых чисел в промежутке 0 до 2^{32} - 1 при помощи встроенного в C++ генератора std::mt_19937.

4.1.6. Требования к статистическим характеристикам

Генерируемые псевдослучайные последовательности должны успешно проходить статистическое тестирование с использованием известной тестовой утилиты PractRand.
Также точки с псевдослучайными координатами, полученными при помощи генератора, при помещении на двумерную плоскость должны равномерно заполнять квадрат (визуальная оценка), углами которого являются точки (a; a) и (b; b), где [a; b] – диапазон генерируемых чисел.

4.2. Требования к математическому обеспечению

В основе псевдослучайного генератора должен лежать алгоритм Hash_DRBG в соответствии со стандартном Национального института стандартов и технологий США NIST SP 800-90A Rev. 1 [12].

4.3. Требования к надежности

Программа должна стабильно работать на компьютере, технические характеристики которого удовлетворяют системным требованиям.
Ошибочные сценарии:

- В случае ввода некорректных параметров через аргументы командной строки в консоль выводится информация о том, в каком виде задаются параметры, программа завершает свое выполнение. Выводимый текст:
  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 умолчанию 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), параметром 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 целое 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 внешнего завершения процесса, единственная доступная опция при наличии данного параметра – инициализация числом (--seed)
- При использовании несовместимых опций (--bits и --min или --max, --test_mode и любая другая опция, кроме --seed) выводится ошибка. Шаблон ошибки:
  Использованы несовместимые опции <опция 1> и <опция 2>.
- Если указана опция, но не указан ее параметр (кроме --bits и –test_mode), выводится ошибка по шаблону:
  Не указан параметр для опции <опция>.
- При генерации значений в файл программа проверяет доступное место на диске. Если места на диске недостаточно, в консоль выводится ошибка, программа завершает свое выполнение. Текст ошибки:

На диске недостаточно свободного места для генерации значений в файл. Проверьте параметр --length.

– При возникновении ошибок, связанных с получением энтропии от устройства, в консоль выводится краткая информация об ошибке, программа завершает свое выполнение. Текст ошибки:
Возникла ошибка при получении энтропии от устройства. Проверьте соответствие системным требованиям.

4.4. Условия эксплуатации

4.4.1. Требования к квалификации оператора

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

4.5. 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).

4.6. Требования к информационной и программной совместимости

4.6.1. Требования к устройству пользователя

Минимальные требования к ПО для стабильного функционирования программы:

– операционная система Windows (версии XP и старше).

4.6.2. Требования к исходным кодам и языкам программирования

Программа должна быть написана на языке C++17.
В исходном коде программы разрешается использовать:

– стандартную библиотеку языка C++;
– библиотеку OpenSSL с открытым исходным кодом;
– WinAPI и Microsoft CryptoAPI;

5. ТРЕБОВАНИЯ К ПРОГРАММНОЙ ДОКУМЕНТАЦИИ

5.1. Предварительный состав программной документации

1. «Криптографически стойкий генератор псевдослучайных чисел». Техническое задание (ГОСТ 19.201-78).
2. «Криптографически стойкий генератор псевдослучайных чисел». Программа и методика испытаний (ГОСТ 19.301-78).
3. «Криптографически стойкий генератор псевдослучайных чисел». Пояснительная записка (ГОСТ 19.404-79).
4. «Криптографически стойкий генератор псевдослучайных чисел». Руководство оператора (ГОСТ 19.505-79).

Текст программы (ГОСТ 19.401-78) не входит в состав программной документации в соответствии с добровольной распиской о неразглашении конфиденциальной информации от 3 февраля 2022 г.

5.2. Специальные требования к программной документации

Документы к программе должны быть выполнены в соответствии с ГОСТ 19.106-78 и ГОСТами к каждому виду документа (см. п. 5.1.);

Пояснительная записка должна быть загружена в систему Антиплагиат через LMS «НИУ ВШЭ».

Документация и программа сдаются в электронном виде в формате .pdf или .docx. в архиве формата .zip или .rar;

За один день до защиты комиссии все материалы курсового проекта:

– техническая документация,
– исполняемый файл,
– отзыв руководителя,
– лист Антиплагиата

должны быть загружены одним или несколькими архивами в проект дисциплины «Курсовой проект 2021-2022» в личном кабинете в информационной образовательной среде LMS (Learning Management System) НИУ ВШЭ.

6. ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ

6.1. Ориентировочная экономическая эффективность

В рамках данной курсовой работы расчет экономической эффективности не предусмотрен.

6.2. Предполагаемая потребность

Псевдослучайные генераторы широко используются в современном мире:

- криптография;
- вероятностные алгоритмы и структуры данных;
- машинное обучение;
- повседневные задачи (например, определение победителей в розыгрышах).

6.3. Экономические преимущества разработки по сравнению с отечественными и зарубежными образцами или аналогами

Многие популярные генераторы псевдослучайных значений не являются криптографически стойкими. Реализуемый генератор будет криптографически стойким, при этом скорость его работы не будет значительно ниже аналогов, не являющихся криптографически стойкими.

7. СТАДИИ И ЭТАПЫ РАЗРАБОТКИ

7.1. Необходимые стадии разработки, этапы и содержание работ

1. Техническое задание.
   1.1. Обоснование необходимости разработки программы.
      - постановка задачи;
      - изучение существующих решений;
      - выбор и обоснование критериев качества и эффективности разрабатываемой программы.

   1.2. Научно-исследовательские работы.
      - изучение существующих алгоритмов генерации псевдослучайных последовательностей;
      - определение структуры входных и выходных данных;
      - определение требований к техническим средствам.

   1.3. Разработка технического задания.
      - определение требований к разрабатываемой программе;
      - определение стадий, этапов разработки программы и программной документации;
      - согласование и утверждение технического задания.
2. Рабочий проект.
   2.1. Разработка программы.
      - проектирование;
      - программирование;
      - отладка программы.

   2.2. Разработка программной документации.
      - разработка программной документации в соответствии с ГОСТ 19.101-77.

   2.3. Испытание программы.
      - разработка, согласование и утверждение программы и методики испытаний;
      - проведение тестирования в соответствии с программой и методикой испытаний;
      - корректировка разработанного программного продукта и программной документации по результатам проведенных испытаний в случае необходимости.
3. Подготовка и передача программы.
   3.1. Подготовка программы и программной документации для презентации и защиты.
   3.2. Утверждение даты защиты программы.
   3.3. Защита разработанного программного продукта
   3.4. Передача программы и программной документации для дальнейшего сопровождения.

7.2. Сроки и исполнители

Сроки:

1. Февраль 2022: Контрольная точка 1 (должен быть готов проект технического задания).
2. Апрель – июнь 2002: Контрольная точка 2 (защита проекта).

Исполнитель: Камнев Петр Андреевич, студент группы БПИ201 образовательной программы «Программная инженерия» факультета компьютерных наук НИУ ВШЭ.

8. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ

8.1. Виды испытаний

Проводится функциональное тестирование программы, а также статистическое тестирование генерируемых последовательностей при помощи специальной утилиты, визуальная оценка равномерности распределения при помещении точек с псевдослучайными координатами на двумерную плоскость. Контроль осуществляется в соответствии с документом «Программа и методика испытаний» (ГОСТ 19.301-79).

8.2. Общие требования к приемке работы

Прием будет произведен при полном соответствии программы требованиям, описанным в пунктах 4.1.1-4.1.5, а также при наличии полного комплекта документации, описанного в разделе 5 настоящего технического задания.

ПРИЛОЖЕНИЕ 1

ТЕРМИНОЛОГИЯ

Криптография – инженерно-техническая дисциплина, которая занимается математическими методами защиты информации [13, с. 16].

Псевдослучайная последовательность – последовательность чисел, которая была вычислена по некоторому определённому арифметическому правилу, но имеет все свойства случайной последовательности чисел в рамках решаемой задачи.

Криптографически стойкий генератор – это генератор псевдослучайных чисел с определёнными свойствами (непредсказуемость, неотличимость от истинно случайного, большой период, эффективность), позволяющими использовать его в криптографии.

Бит – единица измерения количества информации.

Равномерное распределение (дискретной случайной величины) – принимает конечное число n значений с равными вероятностями, соответственно, вероятность каждого значения равна $\frac{1}{n}$

Энтропия (в контексте разработки генератора) – неопределенность (непредсказуемая информация), полученная программой для инициализации псевдослучайного генератора.

Статистическое тестирование – совокупность методов определения меры близости заданной псевдослучайной последовательности к случайной.

Ключи криптографии – секретная информация, используемая криптографическим алгоритмом при зашифровании/расшифровании сообщений, постановке и проверке цифровой подписи и в других криптографических целях.

Командная строка – это текстовый интерфейс между человеком и компьютером, в котором инструкции компьютеру даются путём ввода с клавиатуры текстовых строк (команд).

ПРИЛОЖЕНИЕ 2

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1) ГОСТ 19.102-77 Стадии разработки. Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
2) ГОСТ 19.101-77 Виды программ и программных документов. Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
3) ГОСТ 19.103-77 Обозначения программ и программных документов. Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
4) ГОСТ 19.104-78 Основные надписи. Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
5) ГОСТ 19.105-78 Общие требования к программным документам. Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
6) ГОСТ 19.106-78 Требования к программным документам, выполненным печатным способом. Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
7) ГОСТ 19.201-78 Техническое задание. Требования к содержанию и оформлению. Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
8) ГОСТ 19.603-78 Общие правила внесения изменений. Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
9) ГОСТ 19.604-78 Правила внесения изменений в программные документы, выполненные печатным способом. Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
10) ГОСТ 19.602-78 Правила дублирования, учета и хранения программных документов, выполненных печатным способом. Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
11) ГОСТ 19.301-79 Программа и методика испытаний. Требования к содержанию и оформлению. Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
12) National Institute of Standards and Technology Special Publication 800-90A Revision 1. doi:10.6028/NIST.SP.800-90Ar1.
13) Введение в криптографию / Под общ. ред. В. В. Ященко. — 4-е изд., доп. М.: МЦНМО, 2012. — 348 с.

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 ТЗ 01-1				
Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата