О ПРОГРАММНЫХ РЕАЛИЗАЦИЯХ ТЕСТОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Самойлов Е.И., Благовисная А.Н.
Оренбургский государственный университет

Тестирование последовательностей псевдослучайных чисел, генерируемых с целью использования их в криптографических конструкциях, является одной из важных задач, возникающих при разработке систем обеспечения информационной безопасности. Исследования, имеющие целью совершенствование криптографических средств, являются актуальными и востребованными, поэтому их необходимо отражать в учебных курсах, посвященных криптографическим методам защиты информации.

В учебных дисциплинах, изучающих методы криптографии, вопросы осуществления тестирования псевдослучайных последовательностей можно рассматривать, решая учебные задачи, содержание которых заключается в изучении и применении существующих пакетов тестов к различным видам последовательностей. Особый интерес представляет тестирование последовательностей, выдаваемых генераторами, используемыми в реальных криптосистемах. В этом случае тестирование последовательностей невозможно без применения специальных программных средств, реализующих тестирование. Возникает проблема поиска и выбора готовых программных продуктов, реализующих оценку псевдослучайных последовательностей.

Статистические тесты обычно объединяются в пакеты, представляющие собой подборку различных методик по оценке качества псевдослучайных последовательностей методами статистического анализа. Наиболее распространенными и известными являются пакеты Diehard, TestU01, NIST, CRYPT-X, тесты Д. Кнута. Кроме того, существуют тесты, разрабатываемые исследователями специально для решения особых, специфичных задач, для которых применение стандартных пакетов некорректно или недостаточно для полной и всесторонней оценки качества генерируемых последовательностей.

Рассмотрим существующие статистические тесты псевдослучайных последовательностей с точки зрения их программных реализаций, которые могут быть использованы в учебном процессе.

Пакет Diehard представляет собой набор статистических тестов для измерения качества набора случайных чисел. Автором тестов является Джордж Марсалья, который разрабатывал их в течение нескольких лет и опубликовал в 1995 году на CD-ROM, посвящённом случайным числам. Содержимое CD-ROM находится в открытом доступе на сайте https://web.archive.org/web/20160125103112/http://stat.fsu.edu/pub/diehard/. Он содержит 4,8 миллиарда случайных бит, поделенных на 60 файлов по десять мегабайт. Еще три файла двоичных последовательностей представляют собой типичный выход наиболее распространенных на тот момент коммерческих

ГПСП. Так же CD-ROM содержит сам пакет статистического тестирования Diehard. Каждый тест представлен в виде исходного кода на языках программирования C и Fortran.

Существует реализация пакета Diehard на языке программирования Java [1]. В отличие от оригинальной реализации 1995 года, эта программа имеет графический интерфейс. Вид диалогового окна программы представлен на рисунке 1.

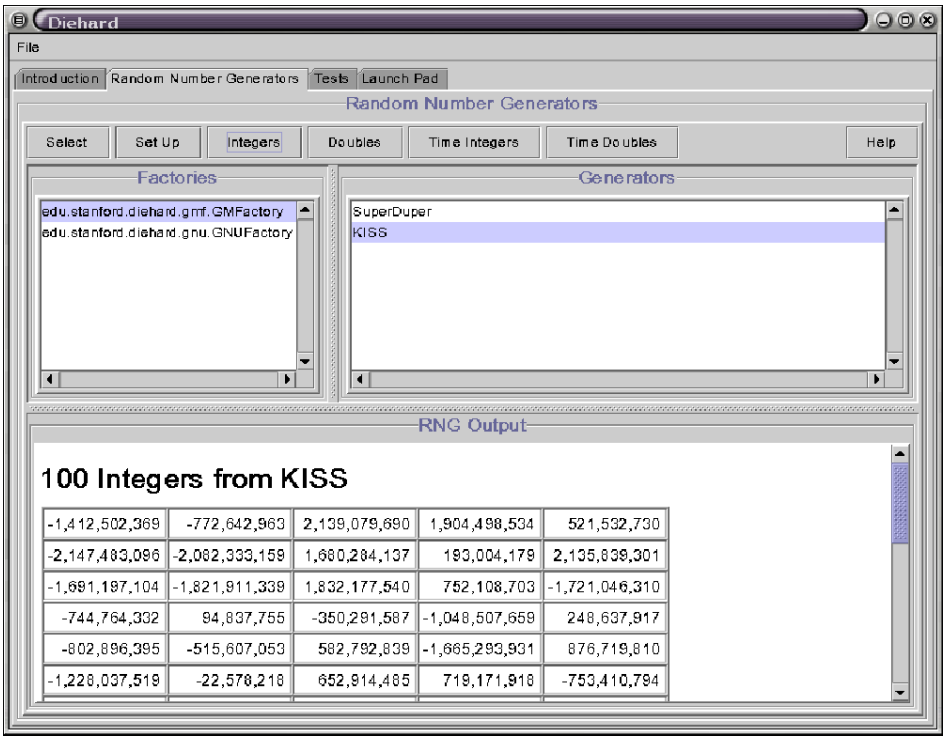

Рисунок 1 – Диалоговое окно реализации пакета Diehard

На момент выхода Diehard считался наиболее строгим пакетом статистического тестирования. Из недостатков можно отметить то, что данный пакет не обновлялся с 1998 года.

Тесты пакета Diehard также реализованы в пакете статистического тестирования Dieharder, предложенном профессором Робертом Дж. Брауном. Dieharder также находится в открытом доступе на сайте https://webhome.phy.duke.edu/~rgb/General/dieharder.php. Кроме тестов Diehard этот пакет содержит три теста из пакета NIST STS, а так же несколько тестов, разработанных автором.

Dieharder поставляется в виде установочного файла, который содержит исходный код статистических тестов и инструкции по установке и использованию пакета. Готовая программа имеет консольный интерфейс.

К преимуществам пакета Dieharder, помимо открытого доступа, следует отнести постоянное обновление и поддержку автором. Кроме того, помимо

установочного файла для операционных систем Windows и Linux, Dieharder так же представлен в виде пакета расширений для языка программирования R [2], что может быть удобно для тех, кто использует этот язык в своих исследованиях.

К одной из первых появившихся программных реализаций тестов псевдослучайных последовательностей следует отнести пакет TestU01. Впервые он был реализован в 1985 году на языке Pascal и содержал тесты, предложенные Д. Кнутом во втором томе книги «Искусство программирования». Постепенно в пакет добавлялись новые статистические тесты и реализации генераторов. Пьер Л'Экуйе и Ричард Симмард [3] полностью переработали библиотеку, реализовав ее на языке программирования C, и перевели руководство с французского на английский язык. Теперь пакет тестов TestU01 реализован в виде библиотеки расширений для языка программирования C. Следует отметить, что вся работа по тестированию генераторов псевдослучайных последовательностей происходит непосредственно с кодом.

Достаточно часто существующие разработанные пакеты тестов улучшают в связи с возрастающими требованиями к псевдослучайным последовательностям и вычислительным мощностям. Так, например, в 2012 году румынскими исследователями (Alin Suciu, Radu Alexandru Toma, Kinga Marton) была представлена распараллеленная с помощью стандарта OpenML реализация библиотеки тестов TestU01 [4], которая, при увеличении размера тестируемой последовательности, показывает большую скорость вычислений и обработки данных. Позже, в 2014 эти же исследователи представили распараллеленную версию TestU01 с использованием объектно-ориентированного подхода [5], которая показала еще больший прирост производительности и скорости вычислений. Однако подобные обновления не всегда оказываются в открытом доступе для всех пользователей.

Еще одним популярным пакетом исследования псевдослучайных последовательностей является пакет статистических тестов NIST, разработанный Лабораторией информационных технологий (Information Technology Laboratory), которая входит в состав Национального института стандартов и технологий (NIST) [6].

NIST STS находится в открытом доступе на сайте https://csrc.nist.gov/Projects/Random-Bit-Generation/Documentation-and-Software. Пакет представляет собой 15 статистических тестов, представленных в виде файлов исходного кода на языке программирования C. После компиляции пользователь получает консольное приложение. Вариант программы с графическим интерфейсом пакета NIST найти не удалось.

В 2010 году румынскими исследователями издана статья, посвященная байт-ориентированной реализации пакета NIST [7], которая позволяет тестировать последовательности большого размера (параметры тестирования последовательностей в оригинальном пакете NIST строго ограничены). Тогда же эти исследователи реализовали распараллеленную версию пакета статистического

тестирования NIST [8]. К сожалению, обе эти реализации не доступны для публичного использования. В 2014 году чешскими исследователями предпринята попытка реализовать более быструю версию оригинального статистического пакета [9]. Эта реализация позволяет достичь большей скорости вычислений, к тому же находится в свободном доступе на сайте https://github.com/sysox/NIST-STS-optimised. Она, как и оригинальная реализация NIST STS, состоит из файлов кода на языке программирования C с возможностью получения консольной программы после компиляции.

Существуют и совместные реализации некоторых тестов. Пример такой реализации, включающей в себя пакеты NIST STS и Diehard, можно найти на сайте http://jrandtest.sourceforge.net/. Программный продукт написан на языке Java, имеет графический интерфейс и является свободным программным обеспечением. Недостатком этой реализации является отсутствие некоторых тестов из оригинальных версий пакетов статистического тестирования, а также 2005 год последнего обновления этой программы.

Таким образом, рассмотрение реализаций пакетов тестов псевдослучайных последовательностей позволяет заключить, что, даже если программные продукты относятся к открытому программному обеспечению, их применение требует от пользователя определенных навыков программирования, знания различных сред и языков программирования, а также временных ресурсов, необходимых для освоения программных версий. Кроме того, часть рассмотренных программ уже достаточно давно не обновлялась. Все это может вызывать затруднения при решении задач, возникающих в процессе освоения разделов учебных дисциплин, связанных с оценкой и тестированием псевдослучайных последовательностей криптографических конструкций.

Список литературы

1 Narasimhan B. JDiehard: An implementation of Diehard in Java [Электронные ресурс] / B. Narasimhan // Proceedings of the 2nd InternationalWorkshop on Distributed Statistical Computing March 15–17, Vienna, Austria. – 2001. – Режим доступа: https://www.r-project.org/conferences/DSC-2001/Proceedings/Narasimhan.pdf

2 Eddelbuettel D. RDieHarder: An R interface to the DieHarder suite of Random Number Generator Tests [Электронные ресурс] / D. Eddelbuettel, Robert G. Brown. – 2014. – Режим доступа: https://cran.r-project.org/web/packages/RDieHarder/ vignettes/ RDieHarder.pdf

3 L'Ecuyer P. TestU01: A C library for empirical testing of random number generators [Электронные ресурс] / P. L'Ecuyer, R. Simard // ACM Transactions on Mathematical Software. – 2007. – No. 4, Vol. 33. – P. 22–40. – Режим доступа: https://www.iro.umontreal.ca/~lecuyer/myftp/papers/testu01.pdf

4 Suciu A. A parallel implementation of the TestU01 statistical test suite / A. Suciu, R. A. Toma, K. Marton // IEEE International Conference on Intelligent Computer Communication and Processing, Cluj-Napoca. – 2012, – P. 317–322.

5 Suciu A. Parallel object-oriented implementation of the TestU01 statistical test suite / A. Suciu, R. A. Toma, K. Marton // IEEE International Conference on Intelligent Computer Communication and Processing, Cluj-Napoca. – 2014. – P. 311–315.

6 A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, Version STS-2.1 [Электронный ресурс] / A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo // NIST Special Publication. – 2010. – Режим доступа: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf

7 Suciu A. Byte-oriented Efficient Implementation of the NIST Statistical Test Suite [Электронный ресурс]/ A. Suciu, K. Marton, I. Nagy, I. Pinca, // IEEE International Conference on Automation, Quality and Testing, Robotics. – 2010. – Режим доступа: https://www.researchgate.net/publication/232628446_Byte-oriented_efficient_implementation_of_the_NIST_statistical_test_suite

8 Suciu A. Parallel Implementation of the NIST Statistical Test Suite / A. Suciu, K. Marton, I. Nagy, I. Pinca // IEEE International Conference on Intelligent Computer Communication and Processing, Cluj-Napoca. – 2010. – P. 363–368.

9 Sýs M. Faster randomness testing with the NIST statistical test suite / M. Sýs, Z. Říha // International Conference on Security, Privacy, and Applied Cryptography Engineering, Springer, Heidelberg. – 2014. – P. 272–284.