УДК 681.322

А.Г. Проценко, И.В. Лысенко

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков

ТЕСТИРОВАНИЕ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ СИСТЕМ ПРОГРАММИРОВАНИЯ НА ОСНОВЕ СТАНДАРТА FIPS140-1

Разработана программа, позволяющая производить оценку битовых псевдослучайных последовательностей на предмет соответствия стандарту FIPS 140-1, и исследованы генераторы псевдослучайных последовательностей систем программирования .NET C#, JAVA, C++.

Ключевые слова: *генераторы псевдослучайных чисел, тесты проверки качества, системы программирования.*

Введение

Постановка задачи. Общеизвестно, что случайные и псевдослучайные числа с требуемыми характеристиками (свойствами) находят широкое применение в различных областях инженерной и исследовательской деятельности. Примером тому является статистическое (имитационное) моделирование систем (процессов).

Что же касается криптографической защиты данных, то в этой сфере псевдослучайные последовательности (ПСП) бит играют, можно сказать без преувеличения, ключевую роль (парольная защита, векторы инициализации во всевозможных приложениях, ключи блочных симметричных криптоалгоритмов, алгоритмы поточного шифрования).

В этой связи к генераторам ПСП бит, применяемым для решения задач защиты информации, предъявляются особые требования.

К их числу относится, например, требование непредсказуемости вправо (влево), заключающееся в невозможности установить с вероятностью, отличной от 0,5, очередной (предыдущий) бит ПСП при известных предыдущих (последующих) значениях бит ПСП [1].

Генераторы ПСП, удовлетворяющие этому требованию, считаются криптографически стойкими [2]. В настоящее время существует немало таких генераторов ПСП бит, реализованных в соответствии с различными принципами (в основном – на базе блочных криптоалгоритмов и криптостойких хэш-функций). Для оценки качества генераторов ПСП, применяемых в целях защиты данных, используется набор тестов, определяемый стандартом FIPS140-1 [3].

Целью данного исследования являлось выяснение следующего обстоятельства: поскольку практически каждая система программирования имеет встроенный генератор псевдослучайных чисел, возник вопрос о том, насколько формируемые на их основе псевдослучайные последовательности соответствуют требованиям, предъявляемым к криптографически стойким генераторам псевдослучайных последовательностей.

В качестве объектов исследования были выбраны распространённые системы программирования Microsoft .NET C# 2008, Sun Java SE 6 и GNU C++ [4, 5].

Методика получения экспериментальных данных

Исследование состояло из нескольких этапов.

1. Подготовка для каждой из систем программирования кодов программ, позволяющих генерировать выборки заданного размера в заданном диапазоне чисел.

2. Генерация исходных данных. Согласно стандарту FIPS140-1 все тестовые операции производятся над потоком данных длиной 20000 бит. Поскольку ни одна тестируемая система программирования не имеет генератора битовых последовательностей, было принято решение интерпретировать результаты работы генераторов псевдослучайных чисел. Каждым генератором псевдослучайных чисел генерировалась последовательность псевдослучайных чисел в диапазоне от 0 до 255, после чего каждое число последовательности интерпретировалось как двоичный набор и записывалось в поток данных побитно. Поскольку десятичное число в диапазоне от 0 до 255 может быть представлено в двоичном коде при помощи 8 символов, для получения тестового потока длиной 20000 бит потребовалась генерация последовательности из 2500 псевдослучайных десятичных чисел.

3. Проверка выборок при помощи тестового приложения, написанного для системы программирования Microsoft .NET C# 2008.

Изложение результатов

В качестве системы программирования для создания тестового приложения была выбрана система программирования Microsoft .NET C# 2008. Данное приложение позволяет проводить исследование встроенного генератора случайных чисел C#, а также генераторов случайных чисел других систем программирования. Проверка генераторов других систем программирования производилась путём анализа данных, сохранённых в текстовый файл.

Генерация последовательностей сисем программирования .NET C# и Java проводилась для операционной системы Microsoft Windows 7 x86. Генерация последовательностей системы программирования C++ производилась для операционной системы Ubuntu Linux 9.10.

Качество генераторов псевдослучайных последовательностей производилось согласно стандарту FIPS140-1. Данный стандарт определяет 4 теста, которые выполняются над последовательностями длиной 20000 бит [2].

1. Монобитный тест. Суть данного теста состоит в подсчёте количества нулей и единиц в последовательности определённой длины. Тест считается пройденным, если количество нулей (n_0) и единиц (n_1) лежит в диапазоне $9654 < n_0\ (n_1) < 10346$. Результаты выполнения теста приведены в табл. 1.

Таблица 1

Результаты монобитного теста

Система программирования	n_0	n_1
.NET C#	9953	10047
JAVA	10013	9987
C++	9949	10051

2. Блоковый тест (тест Покера). Поток данных длиной 20000 бит разбивается на 5000 сегментов по 4 бита каждый, после чего производится подсчёт появлений каждого из сегментов. Обозначим через f(i) количество появлений i-й последовательности ($0 < i < 15$). Тест считается пройденным, если величина X лежит в диапазоне $1{,}03 < X < 57{,}4$, где

$$X = (16/5000) * \left(\sum_{i=0}^{15} [f(i)]^2 \right) - 5000 .$$

Результаты выполнения теста указаны в табл. 2.

Таблица 2

Результаты блокового теста

Система программирования	X
.NET C#	29,9904
JAVA	18,2464
C++	9,2096

3. Тест серий. Под серией понимается последовательность одинаковых символов (нулей или единиц) в исходном потоке данных. Суть теста состоит в проверке количества появления серий определённой длины. Последовательность считается случайной, если появления серий определённой длины лежит в заданных диапазонах. Серия длиной

более 6 бит рассматривается, как серия длиной в 6 бит. Результаты выполнения теста приведены в табл. 3 и 4 (отдельно подсчитано количество серий единиц и нулей).

Таблица 3

Результаты монобитного теста (количество серий единиц)

Система программирования	Длина серии (допустимый диапазон)					
	1 (2267–2733)	2 (1079–1421)	3(502–748)	4 (223–402)	5 (90–223)	>=6 (90–223)
C#	2525	1304	550	298	165	179
JAVA	2632	1228	631	305	151	151
C++	2568	1257	599	301	164	147

Таблица 4

Результаты монобитного теста (количество серий нулей)

Система программирования	Длина серии (допустимый диапазон)					
	1 (2267–2733)	2 (1079–1421)	3(502–748)	4 (223–402)	5 (90–223)	>=6 (90–223)
C#	2520	1282	622	306	124	166
JAVA	2565	1313	622	307	157	134
C++	2555	1248	608	302	141	182

4. Тест длин серий. Суть теста состоит в проверке максимальной длины серии одинаковых элементов. Если последовательность случайна, то максимальная длина серии не должна превышать 34 элемента, т.к. вероятность появления такой серии очень низка. Результаты выполнения этого теста приведены в табл. 5.

Таблица 5

Результаты теста длин серий

Система программирования	Макс. длина серии
.NET C#	15
JAVA	16
C++	11

Выводы

В результате выполнения исследования установлено, что все протестированные системы программирования имеют генераторы псевдослучайных чисел, которые удовлетворяют требованиям стандарта FIPS104-1, т.е. являются криптографически пригодными.

Список литературы

1. Столлингс В. Криптография и защита сетей. Принципы и практика / В. Столлингс. – К.: «Вильямс», 2001. – 669 с.

2. Конеев И.Р. Информационная безопасность предприятия / И.Р. Конеев, А.В. Беляев. – СПб.: БХВ – Петербург, 2003. – 752 с.

3. Federal Information Processing Standards. FIPS PUB 140-1. Security Requirements for Cryptographic Modules. – 1994.

4. Павловская Т.А. С/С++. Программирование на языке высокого уровня / Т.А. Павловская. – СПб.: Питер, 2005. – 461 с.

5. Троелсен Э. Язык программирования C# и платформа .NET 2.0 / Э. Троелсен. – М.: Вильямс, 2007. – 1168 с.

Поступила в редколлегию 15.03.2010

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

ТЕСТУВАННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ СИСТЕМ ПРОГРАМУВАННЯ НА ОСНОВІ СТАНДАРТУ FIPS 140-1

О.Г. Проценко, І.В. Лисенко

Розроблено програму, що дозволяє здійснювати оцінку бітових псевдовипадкових послідовностей з точки зору відповідності стандарту FIPS 140-1, і досліджені генератори псевдовипадкових послідовностей систем програмування .NET C#, JAVA, C++.

Ключові слова: *генератори псевдовипадкових чисел, тести перевірки якості, системи програмування.*

TESTING OF THE PSEUDORANDOM NUMBERS GENERATORS OF THE PROGRAMMING SYSTEMS ON THE BASE OF STANDARD FIPS 140-1

O.G. Protsenko, I.V. Lysenko

Program of the testing of the bit pseudorandom generators on the base of standard FIPS 140-1 is considered and pseudorandom generators of the programming systems .NET C#, JAVA, C++ are investigated.

Keywords: *generators of pseudorandom numbers, tests of quality control, systems of programming.*