РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

Рисунок 3 - Диаграмма процессов авторизации пользователя.

Таким образом, полноценная работа пользователя корпоративной образовательной системы требует усилий по разработке схемы модулей процессов клиентской и серверной части. Предлагаемая методика разработки образовательной системы предусматривает работу пользователей как в условиях наличия связи с интернет так и при отсутствии сетевого соединения с ресурсами базы данных, сохраненным в предыдущем сеансе.

Список использовенных источников

1. Мейер Б. Методы программирования: В 2 т. Пер. с фр. Ю. А. Первина / Под ред. А. П. Ер-шова. М.: Мир, 2012.
2. Фаулер М. Архитектура корпоративных программных приложений. М.: Вильямс, 2009.
3. Гамма Э. Приемы объектно-ориентированного проектирования. Паттерны проектирования / Э. Гамма, Р. Хелм, Р. Джонсон, Дж. Влиссидес. СПб.: Питер, 2009. 366 с.

УДК 004.056.55

ОСНОВЫ ПОСТРОЕНИЯ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Тайлақ Бибігүл Елжасқызы
Докторант кафеды ВТ ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – С.К. Атанов

Генератор псевдослучайных чисел (ПСЧ) или псевдослучайных последовательностей (ПСП) - детерминированный алгоритм, генерирующий последовательность чисел, элементы

которой которые почти независимы друг от друга и подчиняются заданному распределению (обычно равномерному).

Последовательность, порождаемая псевдослучайным генератором, может иметь далеко неравномерную плотность распределения, однако, она будет вычислительно неотличима от равномерной плотности.

Определение (псевдослучайный генератор). Пусть функция $l : N \to N$ удовлетворяет условию $1(n) > n$ для всех $n \in N$. Псевдослучайный генератор с растягивающей функцией 1(n) есть детерминированный полиномиальный алгоритм G со следующими свойствами [1]:

1. Для любой $a \in \{0,1\}^*$ имеет место равенство $|G(a)| = l(|a|)$;

2. Вероятностные ансамбли $\prod = G(\mathrm{Pr}_0^n)$ и $\prod_0^{p(n)}$ вычислительно неразличимы для достаточного большого *n*.

Теорема (построение псевдослучайного генератора). Пусть *f* - односторонняя функция, сохраняющая длину, и предикат *b* - крепкое ядро *f*. Тогда $G(a) = b(a)b(f(\alpha))...\ b(f^{l(|a|)-1}(a))$ есть псевдослучайный генератор с растягивающий функцией.

Теорема (существование псевдослучайного генератора). Псевдослучайные генераторы существуют тогда и только тогда, когда существуют односторонние функции.

Генераторы ПСП являются неотъемлемыми и важными элементами любой системы защиты, это обстоятельство подчёркивает известный афоризм Роберта Р. Кавью: «Генерация случайных чисел слишком важна, чтобы оставлять её на волю случая».

Для криптографической защиты данных, передаваемых по телекоммуникационным каналам в распределенных компьютерных сетях они используются для решения следующих задач [2]:

– генерации сеансовых ключей;

– генерации гаммирующих последовательностей при преобразовании информации по схеме, наиболее близкой к схеме абсолютно стойкого шифра;

– хеширования информации;

– построения самосинхронизирующихся поточных шифров;

– формирования ключевой информации, на секретности и качестве которой основывается стойкость криптоалгоритмов;

– формирования случайных запросов при реализации большого числа криптографических протоколов, например протоколов выработки общего секретного ключа, разделения секрета, аутентификации, электронной подписи и др.

Как известно, статистически безопасный генератор ПСП должен удовлетворять следующим требованиям [2]:

– ни один статистический тест не обнаруживает в ПСП каких-либо закономерностей;

– нелинейное преобразование F_k, зависящее от секретной информации (ключа *k*), используемое для построения генератора, обладает свойством «размножения» искажений – все выходные вектора e' возможны и равновероятны независимо от исходного вектора *e*;

– при инициализации случайными значениями генератор порождает статистически независимые ПСП.

При использовании криптографических алгоритмов одной из самых сложных задач является генерация ключей. Здесь основной проблемой является поддержание определенных криптографических свойств создаваемых ключей. Существуют два метода генерации ключей: детерминированный и недетерминированный [3].

В основу недетерминированных методов заложено использование случайных физических процессов, исходы которых могут служить для дальнейшего изготовления ключей. Источники истинно случайных чисел не являются очень распространенными устройствами. Потенциально такими источниками могут быть физические генераторы

шумов, выходные последовательности которых являются случайно распределенными (например, импульсные генераторы, шумящие диоды, газоразрядные лампы, конденсаторы с утечкой тока и т.д.). Снятые с этих приборов сигналы оцифровываются и представляются в виде двоичных последовательностей для дальнейшего побитового сложения в потоковых шифраторах или служат исходной последовательностью для формирования ключей. Однако применяются такие устройства в приложениях сетевой безопасности крайне редко, т.к. существуют проблемы, связанные как со случайностью, так и с точностью получаемых чисел, не говоря уже о сложностях подключения такого рода устройств к каждой системе в сети. Возможны также грубые атаки на подобные устройства.

Альтернативным решением является создание некоторого набора из большого числа случайных чисел и опубликование его в некотором словаре. Тем не менее, и такие наборы обеспечивают очень ограниченный источник чисел по сравнению с тем количеством, которое требуется приложениям сетевой безопасности. Хотя наборы из этих книг действительно обеспечивает статистическую случайность, они не достаточно случайны, т.к. противник может получить копию словаря.

Поэтому криптографические приложения обычно используют алгоритмические методы генерации случайных чисел. Эти алгоритмы являются детерминированными и поэтому порождают последовательности чисел, которые статистически не случайны. Однако у хорошего алгоритма порождаемые им последовательности чисел выдерживают многие разумные тесты на случайность.

В основе детерминированных методов лежит формирование из случайной последовательности малой длины псевдослучайной последовательности большей длины, которая не отличалась бы по своим статистическим свойствам от первоначальной. Одним из самых распространенных методов формирования псевдослучайных ключевых последовательностей является использование сдвиговых регистров с линейными обратными связями. Их функционирование описывается линейными рекуррентными соотношениями, применение которых в качестве генераторов псевдослучайных ключевых последовательностей не всегда является допустимым. В связи с этим широкое распространение получили процессы, которые носят псевдослучайный характер и имеют физическую природу (движение мыши, время реакции пользователя на работу с устройствами ввода-вывода и др.)

Никакой детерминированный алгоритм не может генерировать полностью случайные числа, он может только аппроксимировать некоторые свойства случайных чисел. Любой ГПСЧ с ограниченными ресурсами рано или поздно зацикливается, т.е. начинает повторять одну и ту же последовательность чисел. Длина циклов зависит от самого генератора и в среднем составляет около $2^{n/2}$, где n-размер внутреннего состояния в битах, хотя линейные конгруэнтные и LFSR-генераторы обладают максимальными циклами порядка 2^n. Если порождаемая ПСЧ последовательность сходится к слишком коротким циклам, то такой ГПСЧ становится предсказуемым и непригодным для практических приложений.

Большинство простых арифметических генераторов хотя и обладают большой скоростью, но имеют серьёзные недостатки:

- слишком короткий период/периоды;
- последовательные значения не являются независимыми;
- некоторые биты «менее случайны», чем другие;
- неравномерное одномерное распределение;
- обратимость.

Наиболее распространены линейный конгруэнтный метод, метод Фибоначчи с запаздываниями, линейный регистр сдвига с обратной связью LFSR.

Из современных ГПСЧ широкое распространение также получил «вихрь Мерсенна», предложенный в 1997 году Мацумото и Нисимурой. Его достоинствами являются колоссальный период ($2^{19937}-1$), равномерное распределение в 623 измерениях (линейный конгруэнтный метод даёт более или менее равномерное распределение максимум в 5

измерениях), быстрая генерация случайных чисел (в 2-3 раза быстрее, чем стандартные ГПСЧ, использующие линейный конгруэнтный метод). Однако, существуют алгоритмы, распознающие последовательность, порождаемую вихрем Мерсенна, как неслучайную. Это делает вихрь Мерсенна неподходящим для криптографии.

Приведенная выше классификация относится к генерации ключей для симметричных алгоритмов шифрования. Проблема генерации ключей для асимметричных алгоритмов связана с получением больших простых чисел и проверкой их на простоту.

Некоторые типы алгоритмов имеют так называемые слабые ключи, использование которых сильно уменьшает криптографическую стойкость зашифрования на данных ключах. Для алгоритма DES, например, с длиной ключа 56 бит существует 16 слабых ключей. Проверка слабых ключей может производиться как экспериментально, так и посредством анализа используемого алгоритма шифрования.

Чтобы получить линейные последовательности элементов гаммы, длина которых превышает размер шифруемых данных, используются датчики ПСЧ. На основе теории групп было разработано несколько типов таких датчиков.

В настоящее время наиболее доступными и эффективными являются конгруэнтные генераторы ПСП [4]. Генераторы этого класса вырабатывают псевдослучайные последовательности чисел, для которых могут быть строго математически определены такие основные характеристики генераторов как периодичность и случайность выходных последовательностей.

Одним из хороших конгруэнтных генераторов является линейный конгруэнтный датчик ПСЧ, вырабатывающий псевдослучайную последовательность чисел $T(i)$, описываемую соотношением $T(i+1) = (A*T(i)+C) \bmod m$, где A и C - константы, $T(0)$ - исходная величина, выбранная в качестве порождающего числа. Эти три величины и образуют ключ.

Период повторения такого датчика ПСЧ зависит от выбранных значений a и c. Значение m обычно принимается равным 2^n, где n - длина машинного слова в битах. Датчик имеет максимальный период M до того, как генерируемая последовательность начнет повторяться. Необходимо выбирать числа A и C такие, чтобы период M был максимальным. Как показано Д. Кнутом, период повторения последовательности генерируемых чисел будет максимальным тогда и только тогда, когда C - нечетное число и $A \pmod 4 = 1$.

Для шифрования данных с помощью датчика ПСЧ может быть выбран ключ любого размера. Например, пусть ключ состоит из набора чисел $x(j)$ размерностью b, где $j=1, 2, ..., n$. Тогда создаваемую гамму шифра G можно представить как объединение непересекающихся множеств $H(j)$. Такой генератор может быть легко создан как программно, так и аппаратными средствами.

Датчики М-последовательностей или M-последовательности также популярны, благодаря относительной легкости их реализации. M-последовательности представляют собой линейные рекуррентные последовательности максимального периода, формируемые k-разрядными генераторами на основе регистров сдвига. На каждом такте поступивший бит сдвигает k предыдущих и к нему добавляется их сумма по модулю 2. Вытесняемый бит добавляется к гамме.

Строго это можно представить в виде следующих отношений:

$$r_1 := r_0 \quad r_2 := r_1 \quad \ldots \quad r_{k-1} := r_{k-2}$$
$$r_0 := a_0\, r_1 \oplus a_1\, r_2 \oplus \ldots \oplus a_{k-2}\, r_{k-1}$$
$$\Gamma_i := r_{k-}$$

Здесь $r_0\ r_1 \ldots\ r_{k-1}$ - k однобитных регистров, $a_0\ a_1 \ldots\ a_{k-1}$ - коэффициенты неприводимого двоичного полинома степени $k-1$. Γ_i - i-е значение выходной гаммы.

Период M-последовательности исходя из ее свойств равен 2^k-1. Другим важным свойством M-последовательности является объем ансамбля, т.е. количество различных M-последовательностей для заданного k. Эта характеристика приведена в таблице 1:

Таблица 1 - Объем ансамбля *M*-последовательности

k	Объем ансамбля
5	6
6	8
7	18
8	16
9	48
10	60
16	2048

Очевидно, что такие объемы ансамблей последовательности неприемлемы. Поэтому на практике часто используют последовательности Голда, образующиеся суммированием нескольких *M*-последовательностей. Объем ансамблей этих последовательностей на несколько порядков превосходят объемы ансамблей порождающих *M*-последовательностей. Так, при *k*=10 ансамбль увеличивается от 1023 (*M*-последовательности) до 388000.

Также перспективными представляются нелинейные датчики ПСП (например сдвиговые регистры с элементом *И* в цепи обратной связи), однако их свойства еще недостаточно изучены. Возможны и другие, более сложные варианты выбора порождающих чисел для гаммы шифра. В работе [5] рассмотрена такая модель псевдослучайного генератора, построенного на базе хаотической системы.

Список использованных источников

1. Птицын Н. Приложение теории детерминированного хаоса в криптографии – М.: МГТУ им. Н.Э. Баумана, 2002.

2. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. - М.: КУДИЦ-ОБРАЗ, 2003. - 240 с.

3. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. - 448 с.

4. Баричев С.В., Гончаров В.В., Серов Р.Е. Основы современной криптографии. - М.: Горячая линия - Телеком, 2001. - 126 с.

5. Тайлак Б.Е. Модель псевдослучайного генератора, построенного на базе хаотической системы //Труды международной научной конференции «Наука и образование – ведущий фактор стратегии «Казахстан – 2030». Караганда: Изд-во КарГТУ, 2009. - С. 353-355.

УДК 631.5.524.28

МЕТОДОЛОГИЯ ВЫБОРА ЦМР ПРИ ИЗУЧЕНИИ СОСТОЯНИЯ ГИДРОЛОГИЧЕСКИХ ОБЬЕКТОВ

Толыбай Еркебулан Аяпбергенулы

Магистрант 1 курса специальности 6М074400 – «Гидротехническое строительство и сооружения»Таразского государственного университета им. М.Х.Дулати, Тараз, Казахстан

Егенбердиев Нурсултан Талгатович

Магистрант 1 курса специальности 6М080500 – «Водные ресурсы и водопользование» Таразского государственного университета им. М.Х.Дулати, Тараз, Казахстан

Сатаев Думан

Магистрант 1курса специальности 6М074400 – «Гидротехническое строительство и сооружения»Таразского государственного университета им. М.Х.Дулати, Тараз,Казахстан

Научные руководители – д.т.н, профессор Сенников М.Н., д.т.н, доцент Омарова Г.Е.