Лабораторная работа № 7

Тема: Поточные шифры и генераторы псевдослучайных чисел
Цель: Изучить применение методов генерации ПСЧ
Пояснения к работе:

Генераторы псевдослучайных чисел могут работать по разным алгоритмам. Одним из простейших генераторов является так называемый линейный конгруэнтный генератор, который для вычисления очередного числа ki использует формулу ki=(a*ki-1+b)mod c, где a, b, c — некоторые константы, a ki-1 — предыдущее псевдослучайное число. Для получения k1 задается начальное значение k0. Возьмем в качестве примера a=5,b=3,c=11 и пусть k0= 1. В этом случае мы сможем по приведенной выше формуле получать значения от 0 до 10 (так как c = 11). Вычислим несколько элементов последовательности:
k1 = (5 * 1 + 3) mod 11 = 8;
k2 = (5 * 8 + 3) mod 11 = 10;
k3 = (5 * 10 + 3) mod 11 = 9;
k4 = (5 * 9 + 3) mod 11 = 4;
k5 = (5 * 4 + 3) mod 11 = 1.
Полученные значения (8, 10, 9, 4, 1) выглядят похожими на случайные числа. Однако следующее значение k6 будет снова равно 8:

Метод Фибоначчи с запаздыванием
Известны разные схемы использования метода Фибоначчи с запаздыванием. Один из широко распространённых фибоначчиевых датчиков основан на следующей рекуррентной формуле:

$$k_i = \begin{cases} k_{i-a} - k_{i-b}, & \text{если } k_{i-a} \geq k_{i-b} \\ k_{i-a} - k_{i-b} + 1, & \text{если } k_{i-a} < k_{i-b} \end{cases}$$

где ki — вещественные числа из диапазона [0,1], a, b — целые положительные числа, параметры генератора. Для работы фибоначчиеву датчику требуется знать max{a,b} предыдущих сгенерированных случайных чисел. При программной реализации для хранения сгенерированных случайных чисел необходим некоторый объем памяти, зависящих от параметров a и b.

Пример.
Вычислим последовательность из первых десяти чисел, генерируемую методом Фибоначчи с запаздыванием начиная с k5 при следующих исходных данных: a = 4, b = 1, k0=0.1; k1=0.7; k2=0.3; k3=0.9; k4=0.5:

k5 = k1 - k4 = 0.7 - 0.5 = 0.2;
k6 = k2 - k5= 0.3 - 0.2 = 0.1;
k7 = k3 - k6 = 0.9 - 0.1 = 0.8;
k8 = k4 - k7 + 1 =0.5 - 0.8 + 1 = 0.7;
k9 = k5- k8 + 1 =0.2 - 0.7 + 1 = 0.5;
k10 = k6 - k9 + 1 =0.1 - 0.5 + 1 = 0.6;
k11 = k7 - k10 = 0.8 - 0.6 = 0.2;
k12 = k8 - k11 = 0.7 - 0.2 = 0.5;
k13 = k9 - k12 + 1 =0.5 - 0.5 + 1 = 1;
k14 = k10 - k13 + 1 =0.6 - 1 + 1 = 0.6.

Видим, что генерируемая последовательность чисел внешне похожа на случайную. И действительно, исследования подтверждают, что получаемые случайные числа обладают хорошими статистическими свойствами.

Широкое распространение получил алгоритм генерации псевдослучайных чисел, называемый алгоритмом BBS (от фамилий авторов — L. Blum, M. Blum, M. Shub) или генератором с квадратичным остатком. Для целей криптографии этот метод предложен в 1986 году.

Вначале выбираются два больших простых числа p и q. Числа p и q должны быть оба сравнимы с 3 по модулю 4, то есть при делении p и q на 4 должен получаться одинаковый остаток 3. Далее вычисляется число M = p* q, называемое целым числом Блюма. Затем выбирается другое случайное целое число x, взаимно простое (то есть не имеющее общих делителей, кроме единицы) с M. Вычисляем x0= x^2mod M. x_0 называется стартовым числом генератора.

На каждом n-м шаге работы генератора вычисляется $x_{n+1}= x_n^2$ mod M. Результатом n-го шага является один (обычно младший) бит числа x_{n+1}. Иногда в качестве результата принимают бит чётности, то есть количество единиц в двоичном представлении элемента. Если количество единиц в записи числа четное – бит четности принимается равным 0, нечетное – бит четности принимается равным 1.

Пример

Пусть p = 11, q = 19 (убеждаемся, что 11 mod 4 = 3, 19 mod 4 = 3). Тогда M = p* q = 11*19=209. Выберем x, взаимно простое с M: пусть x = 3. Вычислим стартовое число генератора x_0:

$x_0 = x^2 \bmod M = 3^2 \bmod 209 = 9 \bmod 209 = 9.$

Вычислим первые десять чисел x_i по алгоритму BBS. В качестве случайных бит будем брать младший бит в двоичной записи числа x_i:

$x_1=9^2$ mod 209= 81 mod 209= 81	младший бит:	1
$x_2=81^2$ mod 209= 6561 mod 209= 82	младший бит:	0
$x_3=82^2$ mod 209= 6724 mod 209= 36	младший бит:	0
$x_4=36^2$ mod 209= 1296 mod 209= 42	младший бит:	0
$x_5=42^2$ mod 209= 1764 mod 209= 92	младший бит:	0
$x_6=92^2$ mod 209= 8464 mod 209= 104	младший бит:	0
$x_7=104^2$ mod 209= 10816 mod 209= 157	младший бит:	1
$x_8=157^2$ mod 209= 24649 mod 209= 196	младший бит:	0
$x_9=196^2$ mod 209= 38416 mod 209= 169	младший бит:	1
$x_{10}=169^2$ mod 209= 28561 mod 209= 137	младший бит:	1

Задание:

1) Определите последовательность из первых десяти чисел и период линейного конгруэнтного генератора ПСЧ для различных параметров a, b и c (k0 принять равным 0):

   a =5, b =7 и c = 17;

$a = 6$, $b = 3$ и $c = 23$.

2) Вычислите последовательность из десяти чисел, генерируемую методом Фибоначчи с запаздыванием начиная с ka при следующих исходных данных:

   $a = 3$, $b = 1$, $k0=0.6$; $k1=0.3$; $k2=0.5$;

   $a = 4$, $b = 2$, $k0=0.9$; $k1=0.3$; $k2=0.5$; $k3=0.9$.

3) Значения k0, k1, k2, k3, полученные с помощью линейного конгруэнтного генератора, равны: $k0 = 1$, $k1 = 12$, $k2 = 3$, $k3 = 6$. Найдите параметры a, b и c генератора ПСЧ.

4) Вычислить x11 по методу генерации псевдослучайных чисел BBS, если $p = 11$, $q = 19$, $x = 3$.

Содержание отчета: Отчет должен содержать пошаговое решение заданий.

Контрольные вопросы:

1. Какие числа называют "псевдослучайными"?
2. Какими свойствами должен обладать генератор псевдослучайных чисел для использования в криптографических целях?
3. Какие генераторы псевдослучайных чисел Вы можете назвать?
4. Перечислите основные характеристики, достоинства и недостатки каждого из рассмотренных в данной лекции генераторов псевдослучайных чисел.