Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

Тульский государственный университет

КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

МЕТОДЫ КРИПТОГРАФИИ. ГЕНЕРАЦИЯ ПСЕВДОБЕСКОНЕЧНЫХ КЛЮЧЕЙ НА ОСНОВЕ ДАТЧИКОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Лабораторная работа № 2
по курсу «Методы и средства защиты компьютерной информации»

Выполнил: студент группы 220601 _____ Белым А.А.
(подпись)
Проверил: д. т. н., проф. каф. ВТ _____ Данилкин Ф.А.
(подпись)

Тула 2013

Цель работы

Знакомство с методами проектирования датчиков псевдослучайных чисел и генерации псевдобесконечных ключей.

Задание

1) Исследовать равномерность датчика (проверить гипотезу о равномерности распределения совокупности ДСЧ).

2) Определить период ДСЧ для различных параметров.

3) Исследовать автокорреляцию совокупности ДСЧ для различных параметров на глубину 100 отсчетов.

4) Построить гистограмму частоты появления каждого возможного значения совокупности ДСЧ.

Текст программы

Далее представлен текст программы на языке C++, реализующей исследование стандартного ДСЧ стандартной библиотеки Си++.

```
#include <iostream>
#include <cstdlib>
#include <ctime>
#include <vector>
#include <map>
#include <cmath>
#include <string>
#include <mgl2/mgl.h>

using namespace std;

void test1(int n=100,int mod=RAND_MAX,unsigned int seed=time(0)){
    map<int,int> freq;
    srand(seed);
    for(int i=0;i<n;++i){
        ++freq[rand()%mod];
    }
    for(auto i=freq.begin();i!=freq.end();++i){
        cout<<i->first<<": "<<i->second<<endl;
    }
}

void test2(int mod=RAND_MAX,unsigned int seed=time(0)){
    srand(seed);
    int i=1;
    for(int r = rand()%mod;r!=rand()%mod;i++);
    cout<<i<<endl;
}
void test3(int n=100,int mod=RAND_MAX,unsigned int seed=time(0)){
    vector<int> v;
    vector<double> res;
    srand(seed);
    double s1=0,s2=0,avg1=0,avg2=0;
    for(int i=0;i<n;i++){
        int t=rand()%mod;
        v.push_back(t);
```

```
        s1+=t;
    }
    s2=s1;avg1=s1/n;
    for(int i=0;i<n/4;i++){
        v.push_back(rand()%mod);
    }
    for(int i=1;i<=n/4;i++){
        s2+=v[i+n-1]-v[i-1];
        avg2=s2/n;
        double a=0,b=0,c=0;
        for(int j=0;j<n;j++){
            c+=(v[j]-avg1)*(v[i+j]-avg2);
            a+=(v[j]-avg1)*(v[j]-avg1);
            b+=(v[i+j]-avg2)*(v[i+j]-avg2);
        }
        res.push_back(c/sqrt(a*b));
    }
    for(int i=0;i<n/4;i++)
        cout<<i+1<<": "<<res[i]<<endl;
}

void test4(string filename="hist.png",int n=100,int mod=RAND_MAX,unsigned int
seed=time(0)){
    map<int,int> freq;
    vector<int> numbers;
    vector<float> counts;
    srand(seed);
    for(int i=0;i<n;++i){
        ++freq[rand()%mod];
    }
    for(auto i=freq.begin();i!=freq.end();++i){
        numbers.push_back(i->first);
        counts.push_back((float)i->second/n);
    }
    mglGraph gr;
    mglData a,b;
    a.Set(numbers); b.Set(counts);
    gr.SetRange('x',a.Minimal(),a.Maximal()+1);
    gr.SetRange('y',0,b.Maximal());
    mglData hist=gr.Hist(a,b);
    gr.Axis("xy");
    gr.Bars(hist);
    gr.WriteFrame(filename.c_str());
}

int main()
{
    int mod,n; string filename;
    cout<<"Исследование равномерности распределения: "<<endl;
    cout<<"Введите количество отсчетов: "; cin>>n;
    cout<<"Введите модуль генератора: "; cin>>mod;
    test1(n,mod);
    cout<<"Исследование периода: "<<endl;
    cout<<"Введите модуль генератора: "; cin>>mod;
    test2(mod);
    cout<<"Исследование автокорреляции: "<<endl;
    cout<<"Введите количество отсчетов: "; cin>>n;
    cout<<"Введите модуль генератора: "; cin>>mod;
    test3(n,mod);
    cout<<"Построение гистограммы частоты случайных чисел:"<<endl;
    cout<<"Введите количество отсчетов: "; cin>>n;
    cout<<"Введите модуль генератора: "; cin>>mod;
    cout<<"Введите имя файла для гистограммы: ";cin>>filename;
    test4(filename,n,mod);
    return 0;
}
```

Тестовый пример

На рисунке 1 представлен пример работы программы при исследовании равномерности распределения и периода случайных чисел:

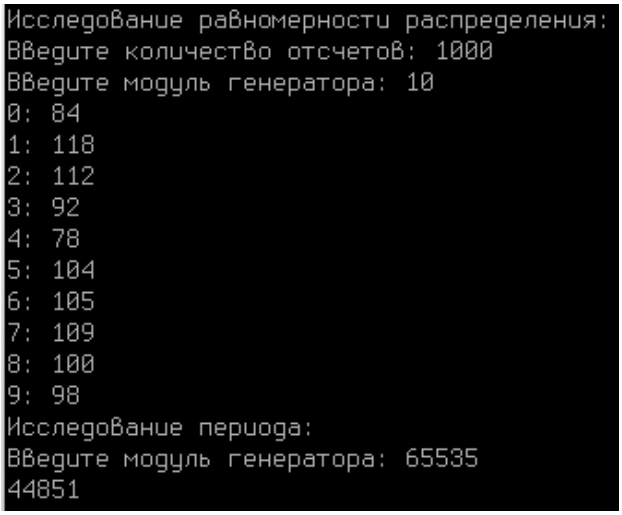

Рисунок 1 – Пример исследования равномерности и периода

На рисунке 2 представлен пример работы программы при исследовании автокорреляции случайных чисел:

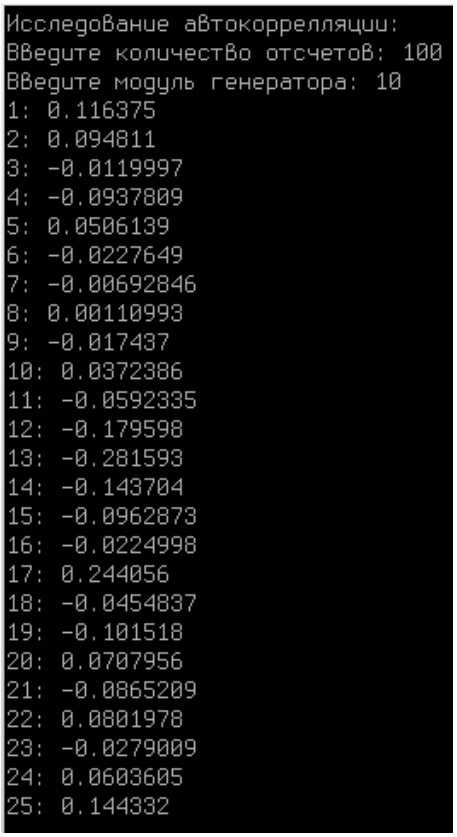

Рисунок 2 – Пример исследования автокорреляции

На рисунке 3 представлен пример работы программы при построении гистограммы частоты полученных случайных чисел:

```
Построение гистограммы частоты случайных чисел:
ВВедите количество отсчетов: 10000
ВВедите модуль генератора: 100
ВВедите имя файла для гистограммы: hist.png
```

Рисунок 3 – Пример построения гистограммы

На рисунке 4 представлена построенная гистограмма:

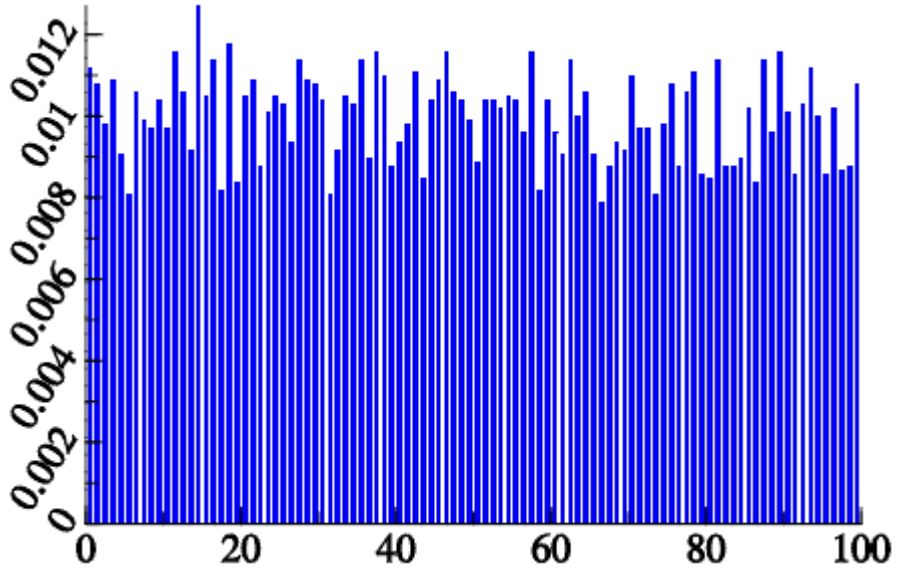

Рисунок 4 – Гистограмма частоты случайных чисел

Вывод

В данной работе я познакомился с принципами построения датчиков псевдослучайных чисел. С помощью псевдослучайных чисел можно получить ключ бесконечной длины, что бывает полезно в некоторых методах криптографии. Была написана программа, которая исследует датчик псевдослучайных чисел стандартной библиотеки языка Си.