Лабораторная работа №5

Вероятностные алгоритмы проверки чисел на простоту

дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Койфман Кирилл Дмитриевич Группа: НФИмд-01-25

Цель работы Получение практических навыков реализации алгоритмов, проверяющих числа на простоту.

Задачи

1. Реализовать алгоритмы проверки чисел на простоту.

---

1 задание

Для решения задачи данной работы была написана программа на C++, реализующая описанные в работе алгоритмы:

```
bool FermTest(int n)
    {
        if (n < 5)
            return false;
        if (n % 2 == 0)
            return false;

        //take random number in [2, n - 2]
        int a = generateRandomInteger(2, n - 2);

        int gamma = static_cast<int>(std::pow(a, n - 1)) % n;

        return gamma == 1 ? true : false;
    }
```

```
    int JacobiSymbolAlgo(int n, int a)
    {
        int g = 1;

        while (true)
        {
            if (a == 0)
                return 0;
            if (a == 1)
                return g;
```

```
            int k = 0;
            int a1 = a;
            while (a1 % 2 == 0)
            {
                a1 /= 2;
                k++;
            }

            int s = 1;
            if (k % 2 != 0)
            {
                if ((n - 1) % 8 == 0 || (n + 1) % 8 == 0)
                {
                    s = 1;
                }
                else if ((n - 3) % 8 == 0 || (n + 3) % 8 == 0)
                {
                    s = -1;
                }
            }

            if (a1 == 1)
                return g * s;

            if ((n - 3) % 4 == 0 && (a1 - 4) % 3 == 0)
            {
                s = -s;
            }

            a = n % a1;
            n = a1;
            g = g * s;
        }
    }
```

```
    bool SolovayShtrassenTest(int n)
    {
        if (n < 5)
            return false;
        if (n % 2 == 0)
            return false;

        int a = generateRandomInteger(2, n - 2);

        int gamma = static_cast<int>(std::pow(a, (n - 1) / 2.0)) % n;

        if (gamma != 1 && gamma != n - 1)
            return false;
```

```
        int s = JacobiSymbolAlgo(n, a);

        if ((gamma - s) % n == 0)
            return false;
        else
            return true;
    }
```

Спасибо за внимание!