Министерство образования Республики Беларусь

Учреждение образования

«Брестский Государственный технический университет»

Кафедра ИИТ

Лабораторная работа №4

По дисциплине «Криптографические методы защиты информации»

Тема: «Тестирование чисел на простоту и построение больших простых чисел»

Выполнил:

Студент 2 курса

Группы ИИ-23

Макаревич Н.Р.

Проверил:

Хацкевич А. С.

Брест 2024

Задание

1. Реализовать приложение, позволяющее генерировать простое число по следующей схеме (с использованием, например, теста Рабина – Миллера):
2. В отчете обязательно должны присутствовать тесты, подтверждающие правильность разработанных программ.

3	Полиномиальный тест распознавания простоты.

Ход работы:

```
bool checkIfPrime(int n) {
    if (n < 2)
        return false;

    std::vector<int> primeNumbers;
    readrimeNumbers(primeNumbers);
    for (int i = 0; i < primeNumbers.size(); i++) {
        if (n == primeNumbers[i])
            return true;
        if (n % primeNumbers[i] == 0)
            return false;
    }

    int r = 1;
    while (r < n) {
        if (findGCD(r, n) != 1)
            return false;
        if (isPrime(r)) {
            int q = findLargestPrimeDivisor(r - 1);
            if (q > 4 * sqrt(r)*log2(n) && (int)pow(n, (r - 1) / q) % r == 1)
                break;
        }
        r++;
    }

    if (r == n)
        return false;

    if (n - 1 <= 2 * sqrt(r) * log2(n)) {
        for (int a = r; a < n; a++)
            if (findGCD(a, n) != 1)
                return false;
    }
    else
        for (int a = 1; a <= 2 * sqrt(r) * log2(n); a++)
            if ((int)pow((3 - a), n) % ((int)pow(3, r) - 1) != (int)pow(3, n) -
a)
                return false;

    return true;
}
```

```
Enter number (0 to exit): 1879
Prime
(Press Enter)
```

```
Enter number (0 to exit): 1515
Complex
(Press Enter)
```

Вывод: в ходе лабораторной работы я освоил алгоритмы проверки числа на простоту.