Математические основы защиты информации и информационной безопасности.

Лабораторная работа №7.

Подмогильный Иван Александрович.

Содержание

List of Figures

List of Tables

1 Цель работы

Освоить на практике вычисление дискретного логарифма методом ро-Полларда

2 Задание

1. Реализовать вычисление дискретного логарифма методом ро-Полларда

3 Выполнение лабораторной работы

Написал код для вычисления дискретного логарифма

```cpp
class DicreteLogarithmHelper {
public:

    static int discreteLogarithm(int a, int b, int m)
    {
        int n = (int) sqrt (m) + 1;

        // Calculate a ^ n
        int an = 1;
        for (int i = 0; i<n; ++i)
            an = (an * a) % m;

        unordered_map<int, int> value;

        // Store all values of a^(n*i) of LHS
        for (int i = 1, cur = an; i<= n; ++i)
        {
            if (! value[ cur ])
                value[ cur ] = i;
            cur = (cur * an) % m;
        }

        for (int i = 0, cur = b; i<= n; ++i)
        {
            // Calculate (a ^ j) * b and check
            // for collision
            if (value[cur])
            {
                int ans = value[cur] * n - i;
                if (ans < m)
                    return ans;
            }
            cur = (cur * a) % m;
        }
        return -1;
    }
```

Figure 3.1: Код для вычисления дискретного логарифма

Код для примеров

```cpp
#include <iostream>
#include "../include/DicreteLogarithmHelper.h"

int main()
{
    int a = 10, b = 64, m = 107;
    cout << DicreteLogarithmHelper::discreteLogarithm(a, b, m) << endl;

    a = 3, b = 7, m = 11;
    cout << DicreteLogarithmHelper::discreteLogarithm(a, b, m) << endl;
}
```

Figure 3.2: Мэйн функция

Вывод примеров

```
/home/pi/education/pfur_masters/matOsnovyInfBez/labs/lab07/cmake-build-debug/main
20
-1

Process finished with exit code 0
```

Figure 3.3: Выовод

4 Выводы

Освоил на практике вычисление дискретного логарифма методов ро-Полларда