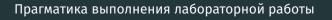
Отчет по лабораторной работе 6

Дисциплина: Математические основы защиты информации и информационной безопасности

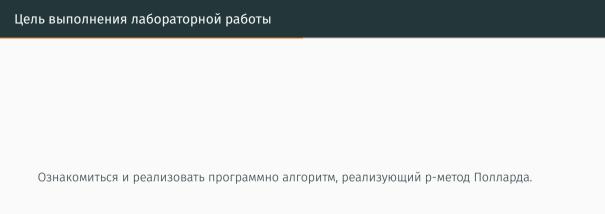
Подмогильный И. А.

25 ноября 2022

Российский университет дружбы народов, Москва, Россия



Приобретение практических навыков разложения чисел на множители.



Реализовать программно алгоритм, реализующий р-метод Полларда

```
#ifndef LAB06 NUMBERDECOMPOSITIONHELPER H
#define LABO6 NUMBERDECOMPOSITIONHELPER H
#include <functional>
#include <GCDHelder.h>
class NumberDecompositionHelper {
    static int pPollardMethod(const int& n. const int& c. std::function<int (int. int)>& cFunc){
        int res, a, b, d;
        a = c \cdot b = c:
        while (true){
            a = cFunc(a, n);
           b = cFunc(b, n):
            GCDHelder::eucBinarv(a - b. n. d):
            if (d > 1.88 d < n){}
                return d:
            else if (d == n){
private:
    static int compressFunc(int x, int modulo){
        return (x*x + 5) % modulo:
```

Задачи выполнения лабораторной работы

Написать функцию мэйн

Figure 2: main

Разложить число на множители



Результатом выполнения работы стала реализация алгоритма нахождения нетривиального делителя, что можно использовать для разложения числа на множители.