Министерство образования Республики Беларусь

Учреждение образования

«Брестский Государственный технический университет»

Кафедра ИИТ

Лабораторная работа №5

По дисциплине «Криптографические методы защиты информации»

Тема: «Факторизация составного числа»

Выполнил:

Студент 2 курса

Группы ИИ-23

Макаревич Н.Р.

Проверил:

Хацкевич А. С.

Брест 2024

Задание

1. Реализовать приложение, позволяющее находить разложение на множители заданного числа n:
   a) методом пробных делений;
   b) согласно заданному варианту;

3	$(p - 1)$ - факторизация Поларда

Ход работы:

```
void trialDivisions(int N) {
    std::ifstream fin;
    fin.open("prime_numbers.txt");
    for (int i = 0; i < 300; i++) {
        int primeNum;
        fin >> primeNum;
        if (N % primeNum == 0)
            std::cout << primeNum << " ";
    }
    fin.close();
}
int pollards_p_minus_1(int n, int B, int a) {
    srand(time(0));
    int g = gcd(a, n);
    if (g > 1) {
        return g;
    }

    for (int j = 2; j <= B; ++j) {
        a = modular_pow(a, j, n);
        g = gcd(a - 1, n);
        if (g > 1 && g < n) {
            return g;
        }
    }

    return -1;
}
```

Разложение числа 287346:

```
Trial divisions method: 2 3 83 577
Pollard: 2 3 6 83 166 498 249 577 3462 1154 1731 47891 95782 143673
```

Вывод: в ходе лабораторной работы я освоил алгоритмы факторизации простых чисел.