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

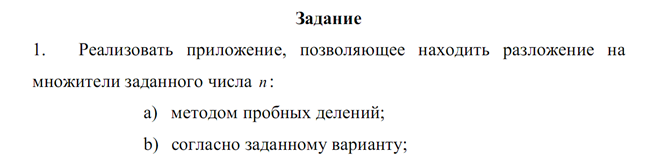
Группы ИИ-23

Макаревич Н.Р.

**Проверил:**

Хацкевич А. С.

Брест 2024



****

**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:

****

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