

# Защита лабораторной 6

по предмету мат. основы защиты информации

---

Дидусь К.В.

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Дидусь Кирилл Валерьевич
- Студент кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов
- 1132223499@rudn.ru
- <https://github.com/kirilldi/>

## Введение

---

- Изучение базовых принципов шифрования
- Важность знания основ шифрования для работы в сфере информационных технологий

Целью данной лабораторной работы является ознакомление с алгоритмом по разложению числа на множители.

- ТУИС РУДН
- Язык программирования Python

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s},$$

Figure 1: Рис. 1. Формула разложения



В ходе выполнения лабораторной работы было реализован алгоритм для разложения заданного числа на 2 нетривиальных сомножителя. Он реализует р-метод Полларда.

Программный код представлен в качестве листинга в конце отчета.

Таким образом, была достигнута цель, поставленная в начале лабораторной работы: я ознакомился с алгоритмом для разложения заданного числа на 2 нетривиальных сомножителя, а так же мне удалось реализовать его на языке программирования Python.