Презентация по лабораторной работе №6

Дисциплина “Математические основы защиты информации и информационной безопасности”

Живцова А.А.

10 октября 2024

Кафедра теории вероятностей и кибербезопасности, Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

Информация

Докладчик

- Живцова Анна Александровна
- студент кафедры теории вероятностей и кибербезопасности
- Российский университет дружбы народов имени Патриса Лумумбы
- zhivtsova_aa@pfur.ru
- https://github.com/AnnaZhiv

Вводная часть

Актуальность

Задача разложения на множители – одна из первых задач, использующихся для построения криптосистем с открытым ключем.

Объект и предмет исследования

- Алгоритм факторизации Полладра

Цели и задачи

- Изучить алгоритм факторизации Полладра
- Реализовать алгоритм факторизации Полладра

Материалы и методы

- Язык программирования Python

Результаты

Тестирование написанной функции

```
poladr(1359331, 1, func, 1, 1)
```

```
1 1 0
6 41 -1
41 123939 -1
1686 391594 -1
123939 438157 -1
435426 582738 -1
391594 1144026 -1
1090062 885749 1181

1181
```

```
1359331/1181
```

```
1151.0
```