Презентация по лабораторной работе №7

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 дискретного логарифмирования в конечном поле – одна из первых задач, использующихся для построения криптосистем с открытым ключем. Эта задача также используется для установления сеансового ключа. Криптоскойкость данных схем основывается на вычислительной сложности решения задачи дискретного логарифмирования.

Объект и предмет исследования

- Алгоритм Полладра для дискретного логарифмирования в конечном поле

Цели и задачи

- Изучить алгоритм Полладра для дискретного логарифмирования в конечном поле
- Реализовать алгоритм Полладра для дискретного логарифмирования в конечном поле

Материалы и методы

- Язык программирования Python

Результаты

Тестирование написанной функции

```
disk_log(107, 10, 64, func, 2, 2)
```

```
4 [2, 2] 4 [2, 2]
40 [3 2] 79 [4 2]
79 [4 2] 56 [5 3]
27 [4 3] 102 [6 4]
56 [5 3] 10 [7 5]
53 [5 4] 87 [8 6]
102 [6 4] 40 [9 7]
1 [6 5] 27 [10  8]
10 [7 5] 53 [11  9]
100 [8 5] 1 [12 10]
87 [8 6] 100 [14 10]

20
```

```
(10**20)%107
```

```
64
```