Презентация лабораторной работы № 7. Дискретное логарифмирование в конечном поле

дисциплина: Математические основы защиты информации и информационной безопасности

Наливайко Сергей Максимович

Цель работы

Цель работы

Познакомиться с дискретным логарифмированием в конечном поле и реализовать алгоритм, реализующий p-метод Полларда.

Задание

- Реализовать алгоритм, реализующий p-метод Полларда для задач дискретного логарифмирования.

Выполнение лабораторной работы

Реализация алгоритма дискретного логарифмирования

```
sergey@sergey: ~/University/math_security/lab07/src
File  Edit  View  Search  Terminal  Help
sergey@sergey:~/University/math_security/lab07/src$ ./main
Введите p: 107
Введите alpha: 10
Введите beta: 64
Введите r: 53
i      c     a1     b1      d     a2     b2
1     40      3      2     79      4      2
2     79      4      2     56      5      3
3     27      4      3     75      5      5
4     56      5      3      3      5      7
5     53      5      4     86      7      7
6     75      5      5     42      8      8
7     92      5      6     23      9      9
8      3      5      7     53     11      9
9     30      6      7     92     11     11
10    86      7      7     30     12     12
11    47      7      8     47     13     13
Уравнение: 7 + 8x ≡ 13 + 13x (mod 53)
Показатель x для выражения (alpha^x - beta) % p == 0 равен 20
sergey@sergey:~/University/math_security/lab07/src$
```

Figure 1: Дискретное логарифмирование в конечном поле

Выводы

Выводы

В ходе работы мы познакомились с дискретным логарифмированием в конечном поле и реализовали алгоритм, реализующий p-метод Полларда.