Математические основы защиты информации и информационной безопасности. Лабораторная работа № 6 на тему “Разложение чисел на множители”

Лубышева Ярослава Михайловна

RUDN University, Moscow, Russian Federation

Содержание

Содержание

Цели и задачи

Цели и задачи

Выполнить задание к лабораторной работе № 6:

1. Ознакомиться с алгоритмом разложения чисел на множители - p-метод Полларда
2. Реализовать алгоритм программно
3. Разложить на множители заданное число

Выполнение

Выполнение

```
# алгоритм Евклида для нахождения НОД
# вход - целые числа 0<b<=a
# выход - d=НОД(a,b)
def alg_Euclid(a, b):
  r = [a, b]
  i = 1
  while r[i-1]%r[i]!=0:
    r.append(r[i-1]%r[i])
    i += 1
  d=r[i]
  return d
```

Figure 1: Программная реализация алгоритма нахождения НОД

Выполнение

```
# p-метод Полларда
# вход: число n, начальное значение c,
# функция f, обладающая сжимающим свойствами
# выход: нетривиальный делитель числа n
def p_method_Pollard(n, c, f):
  a = c
  b = c
  d = 1

  while d == 1:
    a = f(a) % n
    b = f(f(b) % n) % n

    if n <= a-b:
      d = alg_Euclid(abs(a-b), n)
    else:
      d = alg_Euclid(n, abs(a-b))

    if d>1 and d<n:
      return d
    if d == n:
      return "Делитель не найден"
```

Выполнение

```
n = 1359331
c = 1
f = lambda x: (x**2 + 5) % n
print(f"Делитель числа {n} - {p_method_Pollard(n, c, f)}")
```

```
Делитель числа 1359331 - 1181
```

Figure 3: Результаты работы p-метода Полларда

Результаты

Результаты

Выполнено задание к лабораторной работе № 6

Список литературы

Список литературы

1. Методические материалы курса