Лабораторная работа №6

Разложение чисел на множители

Кубасов В.Ю.

Содержание

# 1 Цель работы

Реализовать алгоритм по нахождению нетривиального множителя для заданного числа

# 2 Задание

Реализовать алгоритмы:  
- Алгоритм реализующий p-метод Полларда

# 3 Теоретическое введение

Еще одним вариантом достоверно определить простоту числа - найти для него нетривиальный множитель. Разложение чисел занимает достаточно много времени при условии используемых в шифровании порядков. Однако помимо перебора существуют алгоритмы, оптимизирующие[1] данный процесс.

# 4 Выполнение лабораторной работы

## 4.1 Нахождение НОК

function euklid(a, b)  
 if (a == 0)  
 return 1;  
 end;  
 ri\_1 = a; ri = b; i = 1;  
 while (true)   
 riplus1 = ri\_1 % ri;  
 if (riplus1 == 0)  
 break;  
 end;  
 ri\_1 = ri;  
 ri = riplus1;  
 end;  
 return ri;  
end;

## 4.2 Алгоритм Полларда

function pollard(n, c, func)  
 a = c;  
 b = c;  
 while(true)  
 a = func(a) % n;  
 b = func(func(b) % n) % n;  
 d = euklid(a - b, n);  
 if (1 < d && d < n)  
 return d;  
 end;  
 if (d == n)  
 println("Делитель не найден");  
 return -1;  
 end;  
 end;  
end;

# 5 Выводы:

* В ходе работы реализовали алгоритм оптимального нахождения нетривиальных делителей

# Список литературы

1. Климина А., Жданов О. Оптимизация выбора параметров для алгоритма Полларда // Актуальные проблемы авиации и космонавтики. Федеральное государственное бюджетное образовательное учреждение высшего …, 2011. Т. 1, № 7. С. 424.