Лабораторная работа №6

Математические основы защиты информации и информационной безопасности

Дарижапов Тимур Андреевич

Содержание

# Цель работы

Познакомиться с алгоритмом разбора числа на множители.

# Задание

Реализовать алгоритм, реализующий р-метод Полларда.

# Выполнение лабораторной работы

Данная работа была выполнена на языке Julia.

Для реализации теста Ферма была написана следующая программа (рис. 1 ) :

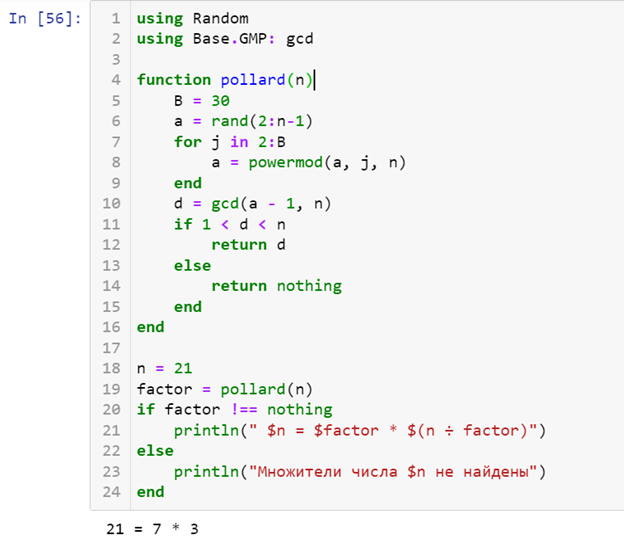


Figure 1: Программа реализации теста Ферма

В данной программе:

1-2 строки: подключение библиотек для случайного числа и для нахождения НОД

4: задание функции

5-9: Задаём сжимающую функцию, в данном случае степенную. Со случайно выбранным числом делаем операцию а^В! mod n.

10: находим НОД чисел а-1 и n

11: проводим проверку условия, если числитель нетривиальный, то выводим его, в ином случае алгоритм необходимо повторить

18: задаём число, которое нужно разложить

19: запускаем функцию.

Мы можем видеть результат на (рис. 1 ) . Программа работает верно.

# Выводы

Познакомился с алгоритмом разбора числа на множители и реализовал алгоритм р-метод Полларда.

# Список литературы

Лабораторная работа №6

Разложение чисел на множители [Электронный ресурс]. URL: https://esystem.rudn.ru/mod/folder/view.php?id=1150978