Математические основы защиты информации и информационной безопасности. Отчет по лабораторной работе №6

Шифрование гаммированием

Попова Юлия

Содержание

# Цель работы

Освоить на практике разложение чисел на множители.

# Выполнение лабораторной работы

Требуется реализовать:

1. Алгоритм, реализующий p-метод Полларда

## p-метод Полларда

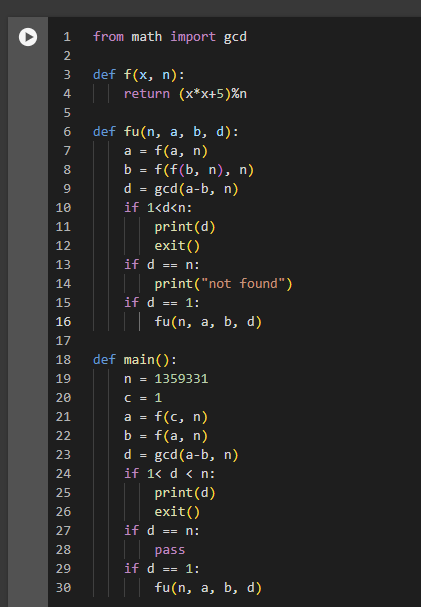
Метод Полларда применяется при факторизации натуральных чисел.

Основные шаги:

Вход: число N, начальное значение c, функция f, обладающая сжимающими свойствами Выход: нетривиальный делительно числа n 1) положить a <- c, b <- c 2) Вычислить a Б- f(a)(mod n), b <- f(b) (mod n) 3) Найти d <- НОД(a-b, n) 4) Если 1< d< n, То положить p <- dи результат: p. При d=n результат: “Делитель не найден”; при d=1 вернуться на шаг 2

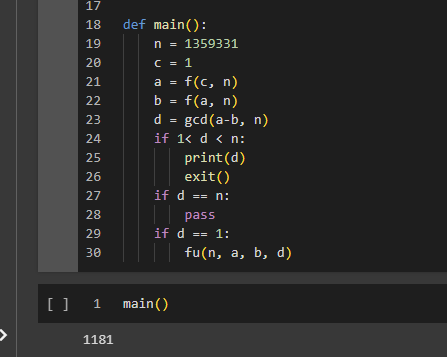
Чтобы реализовать программу, был написан след. код на python:

1. Функция, реализующая p-метод Полларда
2. Функция нахождения НОД [@fig:1].



main\_func

Выходные значения программы (пример из методички) [@fig:2].



output

# Выводы

В результате выполнения работы освоили на практике алгоритм разложения чисел на множители.

# Список литературы

1. Методические материалы курса