Пшенко Артем, ФИТ 3-4

Информационная безопасность

Отчет по лабораторной работе № 3.

Основы теории чисел и их использование в криптографии

Вариант 9

В данной лабораторной работе необходимо было реализовать функцию нахождения простых чисел, а также НОД двух или трех чисел.

Существует множество алгоритмов, позволяющих определить, является ли число простым: малая теорема Ферма, теорема Вильсона, тривиальная проверка на простоту и другие. Воспользуемся последним из перечисленных.

По определению простым называется такое натуральное число n>1, которое делится нацело только на 1 и на само себя. Единица не относится ни к простым, ни к составным числам.

Реализация функции нахождения простых чисел представлена в листинге 1.

Листинг 1. Функция нахождения простых чисел.

|  |
| --- |
| def is\_prime(N):  i = 2  while i <= sqrt(N):  if N % i == 0:  return False  i += 1  return True |

Для вывода простых чисел в консоль в диапазоне [a; b] была реализована соответствующая функция. Исходный код приведен в листинге 2.

Листинг 1. Функция нахождения простых чисел.

|  |
| --- |
| def print\_primes(a, b):  amount = 0  for x in range(a, b + 1):  if(is\_prime(x)):  amount += 1  print(x, end=', ')  print(f'\nКол-во простых чисел в интервале {a, b} равно {amount}') |

Результат работы функций приведен на рисунке 1.



Рисунок 1. Результат работы функций для нахождения простых чисел в диапазоне [2; 433].

Для нахождения НОД двух воспользуемся алгоритмом Евклида. Рассмотрим его на примере.

Если a нацело делится на b, то b и будет являться НОД этих чисел. В остальных случаях для нахождения наибольшего общего делителя двух чисел нужно соблюдать такой порядок действий:

1. Большее число поделить на меньшее.
2. Меньшее число поделить на остаток, который получается после деления.
3. Первый остаток поделить на второй остаток.
4. Второй остаток поделить на третий и т. Д.
5. Деление продолжается до тех пор, пока в остатке не получится нуль. Последний делитель и есть наибольший общий делитель.

Пример 1. Найти наибольший общий делитель чисел 140 и 96.

Как решаем:

1. 140 : 96 = 1 (остаток 44)
2. 96 : 44 = 2 (остаток 8)
3. 44 : 8 = 5 (остаток 4)
4. 8 : 4 = 2

Последний делитель равен 4, это значит НОД (140, 96) = 4. Исходный функции для нахождения НОД двух чисел приведен в листинге 2.

Листинг 2. Исходный функции для нахождения НОД двух чисел.

|  |
| --- |
| Def Euclid(a, b):  while b != 0:  a, b = b, a % b  return a |

Результат работы функции приведен на рисунке 2.



Рисунок 2. Результат работы функций для нахождения НОД на примере чисел 120 и 64.

Таким образом, в данной лабораторной работе были реализованы функции для нахождения простых чисел и НОД, а также были изучены основы теории чисел и их использование в криптографии.