Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

Лабораторная работа №1

«Основы теории чисел и их использование в криптографии»

Студент: Марчук К.С.

ФИТ 3 курс 1 группа

Преподаватель: Копыток Д.В.

Минск 2021

# Цель: приобретение практических навыков выполнения операций с числами для решения задач в области криптографии и разработка приложений для автоматизации этих операций.

# Ход работы

Используя L\_PROST (рисунок 1.1), находим все простые числа в интервале [2, 577]. Количество простых чисел – 102.

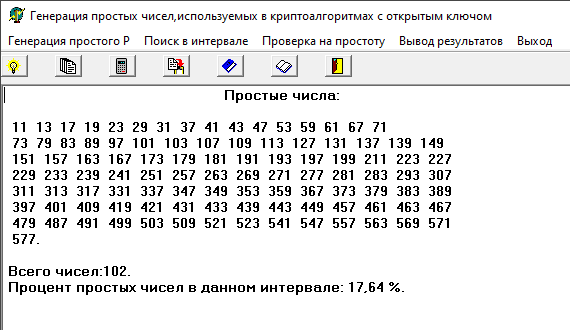


Рисунок 1.1 – Простые числа от 2 до 577 по версии L\_prost

Далее сравним с теоретическим количеством простых чисел, вычисляемым по формуле n/ln(n), где n = 577. Получим 90.75, что почти на 12 меньше, чем полученный программой результат.

Теперь повторим вычисления выше для интервала [540,577]. Результат программы вычислений L\_PROST представлен на рисунке 1.2.

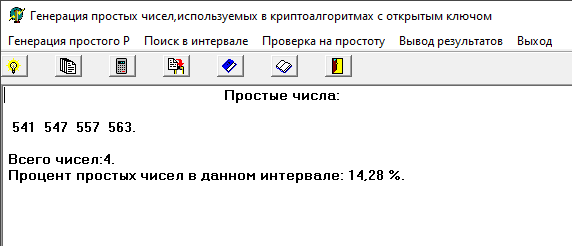


Рисунок 1.2 – Простые числа от 2 до 577 по версии L\_prost

Сравним с теоретическим количеством простых чисел, отняв от предыдущего результат количество простых числе в интервале [2, 540]. Получим 4,925, что соответствует полученному в программе результату.

Результат ручного поиска простых чисел по решету Эратосфена даёт нам иные результаты для второго случая.

m = 540 = 2 \* 2 \* 3 \* 3 \* 3 \* 5.

число n является простым.

m || n = 540577 число является простым.

НОД (540, 577) = 1. Зная, что одно из чисел – простое и не является делителем первого, можно сделать вывод, что НОД этих чисел равен единице.