Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут прикладного системного аналізу

Кафедра математичних методів системного аналізу

**Звіт**

про виконання лабораторної роботи №1

з дисципліни “Безпека інформаційних систем”

Виконав:

Студент 4 курсу

Групи КА-75

Степанюк Владислав Варіант №16

Перевірив:

Мухін В. Є.

Київ – 2020

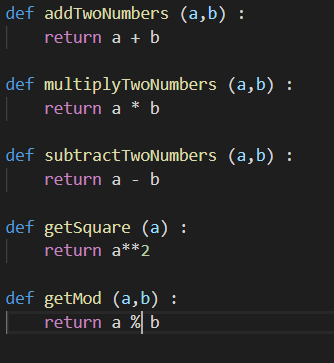
**Завдання**

Розробка програми швидкого дискретного потенціювання (БДП) для виконання обчислювальних операцій в алгоритмах шифрування RSA і El-Gamal і в інших схемах і алгоритмах. Програма повинна реалізувати арифметику (додавання, множення, зведення в квадрат, визначення залишків по модулю) з довгими вихідними числами до декількох десятків (за варіантами) десяткових розрядів.

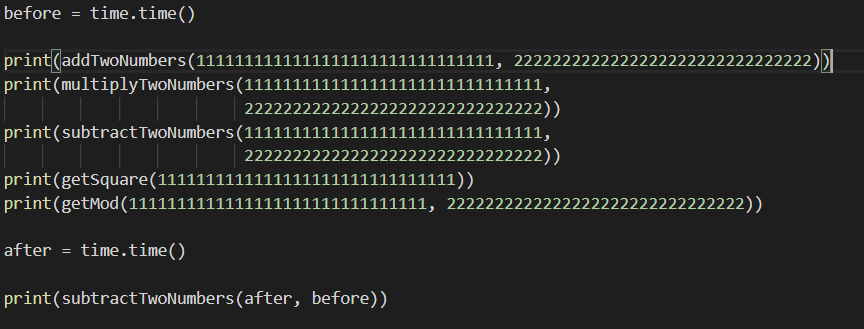
**Обгрунтування вибору прогрманого забеспечення**

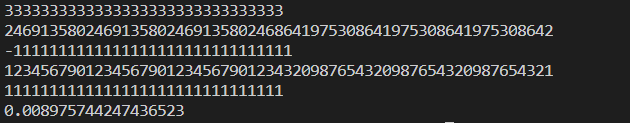
Для виконання цієї лабораторної роботи було вибрано мову програмування Python, так як це елементарна у вивченні мова, що якраз задовільняє вимоги завдання, а саме роботу з великими числами. Тому реалізація стандартної арифметики не забрала багато часу.

**Лістинг коду**



**Результати**





**Висновки**

На виконання цієї програми було витрачено менше однієї сотої секунди, що дуже швидко. Отже, Python - мова що якісно та швидко справляється з операціями над великими числами.