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

```
def addTwoNumbers (a,b) :
    return a + b

def multiplyTwoNumbers (a,b) :
    return a * b

def subtractTwoNumbers (a,b) :
    return a - b

def getSquare (a) :
    return a**2

def getMod (a,b) :
    return a % b
```

Результати

```
before = time.time()

print(addTwoNumbers(11111111111111111111111111111111, 22222222222222222222222222222222))
print(multiplyTwoNumbers(11111111111111111111111111111111,
                         22222222222222222222222222222222))
print(subtractTwoNumbers(11111111111111111111111111111111,
                         22222222222222222222222222222222))
print(getSquare(11111111111111111111111111111111))
print(getMod(11111111111111111111111111111111, 22222222222222222222222222222222))

after = time.time()

print(subtractTwoNumbers(after, before))
```

```
33333333333333333333333333333333
246913580246913580246913580246864197530864197530864197530864 2
-11111111111111111111111111111111
12345679012345679012345679012343209876543209876543209876543 21
11111111111111111111111111111111
0.008975744247436523
```

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.