Національний технічний університет України «КПІ ім. Ігоря Сікорського»
Факультет Інформатики та Обчислювальної Техніки
Кафедра Автоматизованих Систем Обробки Інформації та Управління

Лабораторна робота №4

з дисципліни «Системи Безпеки Програм і Даних»

Виконав:
студент гр. ІС-91
Мягков Герман

Київ – 2021

Зміст

1 Постановка задачі

Лаб. Робота 4.1. Розробка програми швидкого дискретного потенціювання (ШДП) для виконання обчислювальних операцій в алгоритмах шифрування RSA і El-Gamal та в інших схемах і алгоритмах. Програма повинна реалізувати арифметику (додавання, множення, зведення в квадрат, визначення залишків по модулю) з довжиною вихідних чисел до декількох десятків (за варіантами) десяткових розрядів.

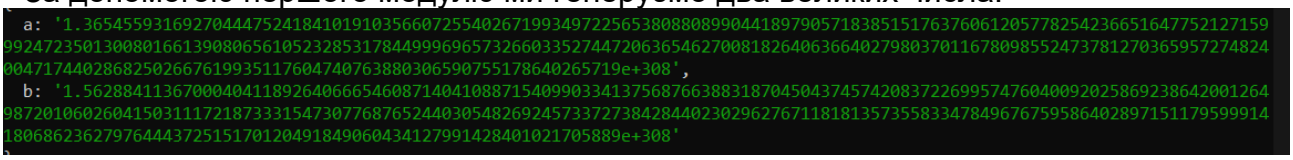
Лаб. Робота 4.2. Розробка програми генератора великих простих чисел (ВПЧ). Для шифрування і розрахунку ключів за схемою RSA необхідно використовувати два великих простих десяткових числа з кількома десятками десяткових розрядів (за варіантами). Для генерації таких простих чисел можна використовувати формули у відповідності з тестом Рабіна або іншими алгоритмами, але для перевірки властивостей сформованих кандидатів у прості числа необхідно використовувати малу теорему Ферма і алгоритм ШДП.

2 Розв’язок

Програма реалізована на язику Javascript за допомогою сторонніх бібліотек («node модулей»):
1) Bignumber. Бібліотека яка реалізує математичні операції над числами з великою кількістю символів:
https://github.com/MikeMcl/bignumber.js/

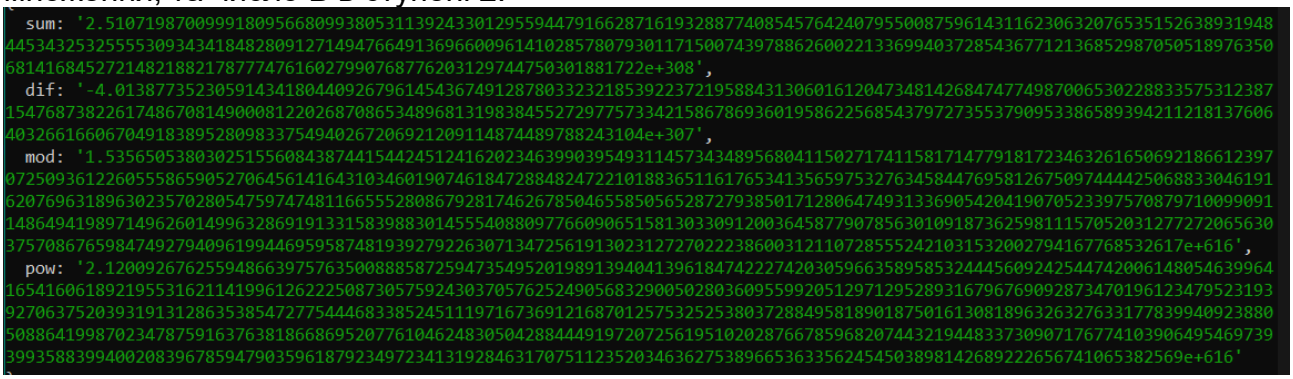
2) Node-forge. Реалізує алгоритми шифрування:
https://github.com/digitalbazaar/forge

- За допомогою першого модулю ми генеруємо два великих числа:



```
  a: '1.365455931692704447524184101910356607255402671993497225653808808990441897905718385151763760612057782542366516477521271599924723501300801661390806561052328531784499969657326603352744720636546270081826406366402798037011678098552473781270365957274824004717440286825026676199351176047407638803065907551786402657 19e+308',
  b: '1.562884113670004041189264066654608714041088715409903341375687663883187045043745742083722699574760400920258692386420012649872010602604150311172187333154730776876524403054826924573372738428440230296276711818135735583347849676759586402897151179599914180686236279764443725151701204918490604341279914284010217058 89e+308'
```


- За допомогою другого модулю демонструємо арифметичні операції над парою чисел. В Нашому випадку це сума чисел А та Б, різниця А та Б, результат їх множення, та число Б в ступені 2:



```
  sum: '2.5107198700999180956680993805311392433012955944791662871619328877408545764240795500875961431162306320765351526389319484453432532555530934341848280912714947664913696600961410285780793011715007439788626002213369940372854367712136852987050518976350681416845272148218821787774761602799076877620312974475030188172 2e+308',
  dif: '-4.013877352305914341804409267961454367491287803323218539223721958843130601612047348142684747749870065302288335753123871547687382261748670814900081220268708653489681319838455272977573342158678693601958622568543797273553790953386589394211218137606403266166067049183895280983375494026720692120911487448978824310 4e+307',
  mod: '1.535650538030251556084387441544245124162023463990395493114573434895680411502717411581714779181723463261650692186612397072509361226055865905270645614164310346019074618472884824722101883651161765341356597532763458447695812675097444425068833046191620769631896302357028054759747481166555280867928174626785046558505652872793850171280647493133690542041907052339757087971009909114864941989714962601499632869191331583988301455540880977660906515813033091200364587790785630109187362598111570520312772720656303757086765984749279409619944695958748193927922630713472561913023127270222386003121107285552421031532002794167768532617e+616',
  pow: '2.120092676255948663975763500888587259473549520198913940413961847422274203059663589585324445609242544742006148054639964165416061892195531621141996126222508730575924303705762524905683290050280360955992051297129528931679676909287347019612347952319392706375203931913128635385472775444683385245111971673691216870125753252538037288495818901875016130818963263276331778399409238805088641998702347875916376381866869520776104624830504288444919720725619510202876678596820744321944833730907176774103906495469739399358839940020839678594790359618792349723413192846317075112352034636275389665363356245450389814268922265674106538256 9e+616'
```

3 Лістинг програми

GitHub:
https://github.com/ldvy/infosec/tree/main/lab4