

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

## Лабораторна робота №5

з дисципліни «Системи Безпеки Програм і Даних»

Виконав:  
студент гр. ІС-91  
Мягков Герман

## **Зміст**

Зміст .....	2
1 Постановка задачі .....	3
2 Розв'язок .....	4
3 Лістинг програми .....	5

## 1 Постановка задачі

**Лаб. Робота 5.** 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 довгою вихідних чисел до декількох десятків (за варіантами) десяткових розрядів.

## 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: '1.3654559316927044475241841019103566072554026719934972256538088089904418979057183851517637606120577825423665164775212715992472350130080166139080656105232853178449996965732660335274472063654627008182640636640279803701167809855247378127036595727482400471744028682502667619935117604740763880306590755178640265719e+308',
b: '1.56288411367000404118926406665460871404108871540990334137568766388318704504374574208372269957476040092025869238642001264987201060260415031117218733315473077687652440305482692457337273842844023029627671181813573558334784967675958640289715117959991418068623627976444372515170120491849060434127991428401021705889e+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: '2.51071987009991809566809938053113924330129559447916628716193288774085457642407955008759614311623063207653515263893194844534325325555309343418482809127149476649136966009614102857807930117150074397886260022133699403728543677121368529870505189763506814168452721482188217877747616027990768776203129744750301881722e+308',
dif: '-4.0138773523059143418044092679614543674912878033232185392237219588431306016120473481426847477498700653022883357531238715476873822617486708149000812202687086534896813198384552729775733421586786936019586225685437972735537909533865893942112181376064032661660670491838952809833754940267206921209114874489788243104e+307',
mod: '1.53565053803025155608438744154424512416202346399039549311457343489568041150271741158171477918172346326165069218661239707250936122605558659052706456141643103460190746184728848247221018836511617653413565975327634584476958126750974444250688330461916207696318963023570280547597474811665552808679281746267850465585056528727938501712806474931336905420419070523397570879710099091148649419897149626014996328691913315839883014555408809776609065158130330912003645877907856301091873625981115705203127727206563037570867659847492794096199446959587481939279226307134725619130231272022386003121107285552421031532002794167768532617e+616',
pow: '2.1200926762559486639757635008885872594735495201989139404139618474222742030596635895853244456092425447420061480546399641654160618921955316211419961262225087305759243037057625249056832900502803609559920512971295289316796769092873470196123479523193927063752039319131286353854727754446833852451119716736912168701257532525380372884958189018750161308189632632763317783994092388050886419987023478759163763818668695207761046248305042884449197207256195102028766785968207443219448337309071767741039064954697393993588399400208396785947903596187923497234131928463170751123520346362753896653633562454503898142689222656741065382569e+616'
```

### **3 Лістинг програми**

GitHub:

<https://github.com/ldvy/infosec/tree/main/lab5>