Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”
НН Фізико-технічний інститут
Дисципліна: “Методи реалізації криптографічних механізмів”

# ЛАБОРАТОРНА РОБОТА №1

**Виконав:**
Студент групи ФБ-21мн

ЩЕРБАКОВ О.К.

Київ – 2023

## Завдання

1. Дослідити алгоритми реалізації арифметичних операцій над великими числами за допомогою бібліотеки багаторозрядної арифметики GNU GMP для паралельної моделі обчислень (x64 розярдність).

# Завдання №1

На [Малюнок 1-4] можна побачити “шлях” виконання завдань, зазначених у методичних вказівках. Код програми можна знайти за посиланням (https://drive.google.com/drive/folders/1x3LKT8J8xF_k991OwOtrU2g82r7htQGc?usp=sharing).

```
Checking 'add' functions...
        [+]: 8373922815996829720 + 9610445676819351714 = 17984368492816181434 (time: 5.387e-06 s.)
        [+]: 2294847108105372040 + 16139184710651068945 = 18434031818756440985 (time: 4.51e-07 s.)
        [+]: 7769011930935564646 + 17725318485259141620 = 25494330416194706266 (time: 7.6e-08 s.)
        [+]: 6198165165928485063 + 6001194125174340111 = 12199359291102825174 (time: 4.6e-08 s.)
        [+]: 14440998793493661893 + 15853084436323703665 = 30294083229817365558 (time: 4.8e-08 s.)
[AVG time]: 1.2016e-06 s. (5.387e-06, 4.51e-07, 7.6e-08, 4.6e-08, 4.8e-08)
```

***Малюнок 1:*** *Вивід консолі під час тестування додавання над цілими числами*

```
Checking 'sub' functions...
        [+]: 836679780903306222 - 12307327551625184597 = -11470647770721878375 (time: 1.458e-06 s.)
        [+]: 15653856951713210637 - 4418005688108974991 = 11235851263604235646 (time: 8.4e-08 s.)
        [+]: 11246114510154525831 - 4136314341248313852 = 7109800168906211979 (time: 3.3e-08 s.)
        [+]: 12921773575259623224 - 12002599063704008911 = 919174511555614313 (time: 3.2e-08 s.)
        [+]: 6285416260547240611 - 9422440949804076359 = -3137024689256835748 (time: 5.6e-08 s.)
[AVG time]: 5.7292e-07 s. (1.458e-06, 8.4e-08, 3.3e-08, 3.2e-08, 5.6e-08)
```

***Малюнок 2:*** *Вивід консолі під час тестування віднімання над цілими числами*

```
Checking 'mul' functions...
       [+]: 4897074960193078580 * 15161780820165741386 = 74248377206369330302245131271456111880 (time: 3.228e-06 s.)
       [+]: 9317895301731162301 * 1037137708227370570 = 9663940578740041266990082467140881570 (time: 9.2e-08 s.)
       [+]: 15508091804283273670 * 12618502534724415757 = 195688895741087426922735843318091218190 (time: 4.2e-08 s.)
       [+]: 10225689266113124945 * 6547633298047772787 = 669540635342919895999546272459018717l5 (time: 3.3e-08 s.)
       [+]: 6425542478325226859 * 4771749667158424987 = 3066108018226072246572932779990912583l (time: 3e-08 s.)
[AVG time]: 7.99584e-07 s. (3.228e-06, 9.2e-08, 4.2e-08, 3.3e-08, 3e-08)
```

***Малюнок 3:*** *Вивід консолі під час тестування множення над цілими числами*

```
Checking 'div' functions...
        [+]: 2885822427146921234 / 1152830883948224047 = 0.2503248714e1 (time: 7.899e-06 s.)
        [+]: 13359206434093913845 / 10867112330011188200 = 0.1229324408e1 (time: 2.39e-07 s.)
        [+]: 6231917821277028398 / 2940888337258905948 = 0.2119059654e1 (time: 9.1e-08 s.)
        [+]: 1906307503789168476 / 17198776412713313717 = 0.1108397166e0 (time: 7.4e-08 s.)
        [+]: 17786543954265115580 / 11649348916219008l2 = 0.15268273e2 (time: 7.9e-08 s.)
[AVG time]: 1.83632e-06 s. (7.899e-06, 2.39e-07, 9.1e-08, 7.4e-08, 7.9e-08)
```

***Малюнок 4:*** *Вивід консолі під час тестування ділення над цілими числами з плаваючою комою*