Національний технічний університет України

«Київський політехнічний інститут»

Факультет інформатики та обчислювальної техніки

Кафедра автоматизованих систем обробки інформації і управління

Лабораторна робота №5

з дисципліни «Безпека програм та даних»

Тема: Розробка програми швидкого дискретного потенціювання

Виконав:

студент групи ІП-21

Кіндзерський О.В.

Перевірив:

Корнага Я.І.

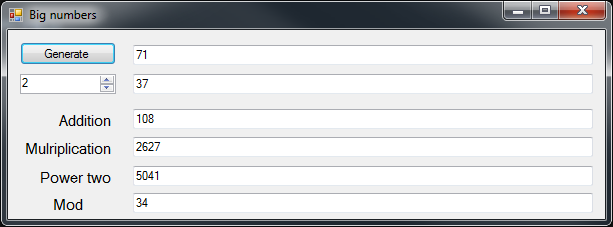
Номер залікової книжки:

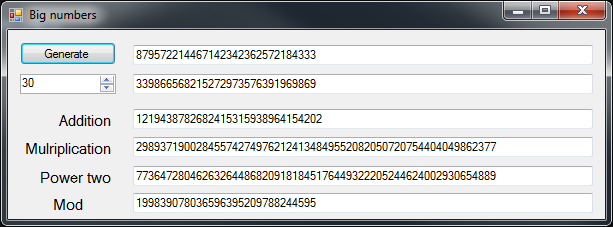
2106

Київ 2015

**Завдання.** Створити програмний макет системи для генерації простих великих простих чисел.

**Результати виконання програми**.





Псевдо код для тесту Рабіна – Міллера:

**Input**: *n* > 3, an odd integer to be tested for primality;

**Input**: *k*, a parameter that determines the accuracy of the test

**Output**: *composite* if *n* is composite, otherwise *probably prime*

write *n* − 1 as 2*r*·*d* with *d* odd by factoring powers of 2 from *n* − 1

WitnessLoop: repeat *k* times:

pick a random integer *a* in the range [2, *n* − 2]

*x* ← *ad* mod *n*

if *x* = 1 or *x* = *n* − 1 then do next WitnessLoop

repeat *r* − 1 times:

*x* ← *x*2 mod *n*

if *x* = 1 then return *composite*

if *x* = *n* − 1 then do next WitnessLoop

return *composite*

return *probably prime*

**Висновок.** На даній лабораторній роботі було розроблено макет системи для генерації простих великих чисел.