МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп’ютерної та програмної інженерії

Кафедра інженерії програмного забезпечення



Лабораторна робота №3

з дисципліни «Безпека ПД»

На тему: «Симетричні системи шифрування»

Варіант №5

Виконав студент:

групи ПІ-421Б

Іванюк Н. О.

Перевірив викладач:

Радішевський М. Ф.

Київ 2022

**Завдання**

Завдання 1. Додати в калькулятор дві операції:

- Перевірку простоти числа на основі теореми Ферма (аргумент – число, результат – просте/ні)

- Генерацію простого числа p A, де А верхня границя (аргумент – границя А, результат – просте число)

**Завдання 2.** Перевірити на основі алгоритму Евкліда взаємну простоту двох пар чисел шляхом визначення їх найбільшого дільника. Номер варіанта = номер студента по списку (mod 7) +1

Варіант: 5mod7 + 1 = **6**

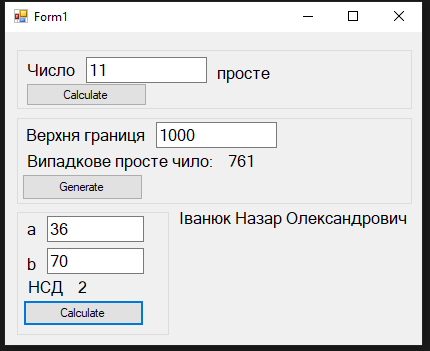
Завдання 3. Реалізувати на калькуляторі алгоритм Евкліда для визначення взаємної простоти чисел. Вхідні параметри числа а та в, результат – загальний дільник

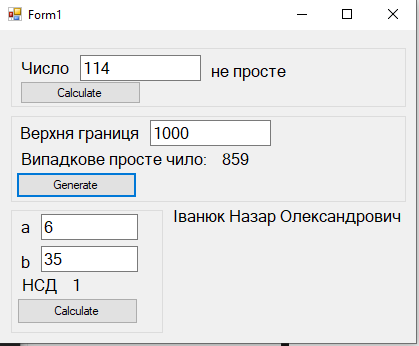
**Виконання роботи**

Реалізація малої теореми Ферма на мові С#:

Math.Pow(a,(p - 1)) % p == 1 – умова простого числа,

при цьому *a* – число в інтервалі [2;p-2], *p* – припустимо просте число.





**Завдання 2**

Варіант 6

1. 36,70

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № кроку |  |  |  | | |  |  |
| a | b | a | g\*b | +r | =0 | переозначення |
| 1 | 70 | 36 | 70 | 1\*36 | +34 | ні | a=36,b=34 |
| 2 | 36 | 34 | 36 | 1\*34 | +2 | ні | a=34,b=2 |
| 3 | 34 | 2 | 34 | 17\*2 | +0 | так | НСД=b=2 |

1. 6,35

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № кроку |  |  |  | | |  |  |
| a | b | a | g\*b | +r | =0 | переозначення |
| 1 | 35 | 6 | 35 | 5\*6 | +1 | ні | a=6,b=1 |
| 2 | 6 | 1 | 6 | 6\*1 | +0 | так | НСД=b=1 |