Лабораторна робота №1

Звіт

З дисципліни “Основи інформаційної безпеки”

МІТ-21, Дашковський Максим

Тема: **«Генерація послідовності випадкових чисел»**

**Завдання 3:**

Написати програму, яка забезпечує генерацію та виведення на екран послідовності псевдовипадкових чисел. Порівняти елементи послідовності для однакових та різних початкових значень. Зробити висновки.

Код програми:

using System;

namespace Lz1\_1

{

internal class Program

{

static void Main(string[] args)

{

Random random = new Random(1234567890);

for (int i = 0; i < 10; i++)

{

int num = random.Next(1, 10);

Console.WriteLine(num);

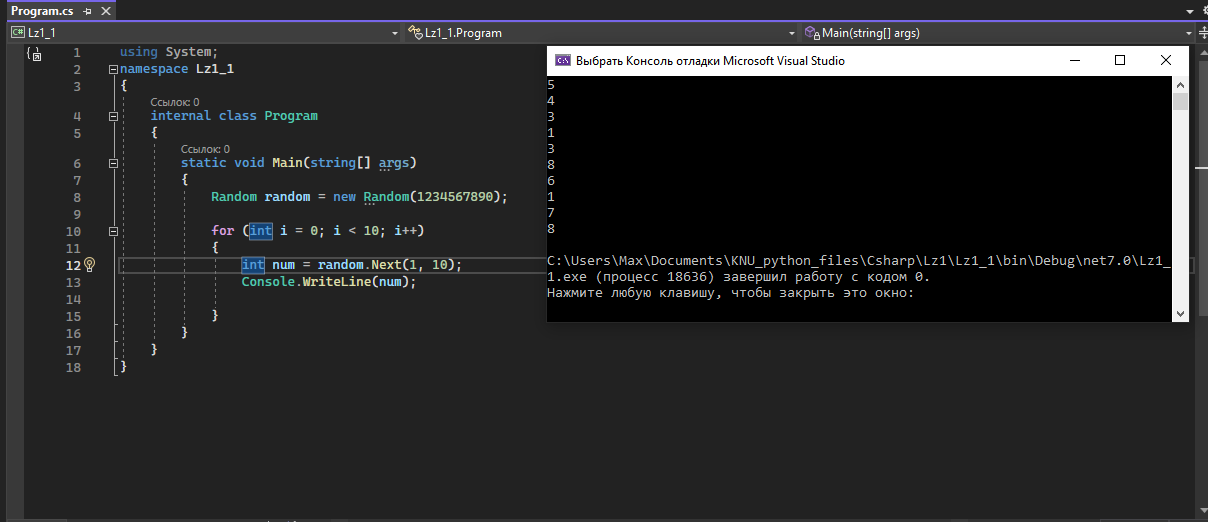
}

}

}

}

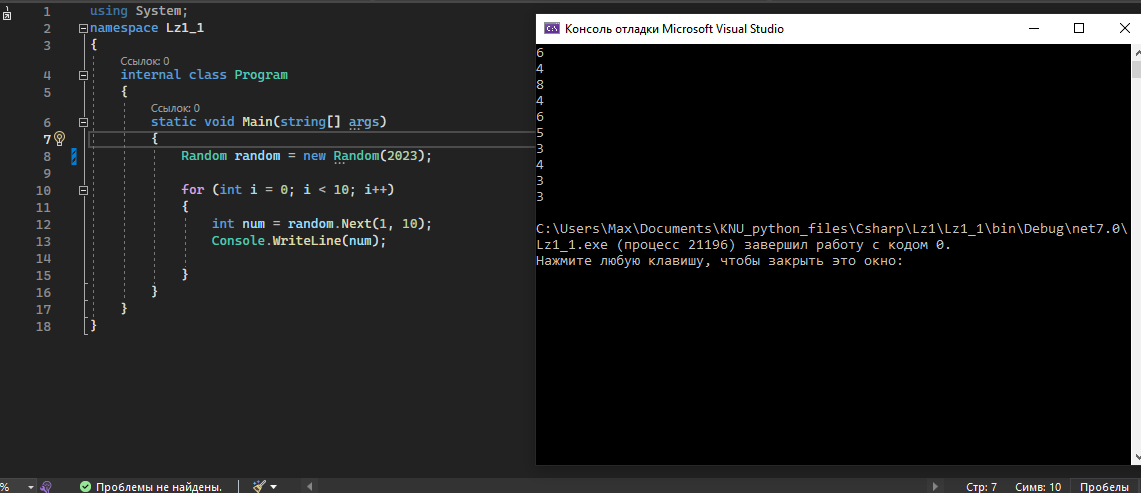
При запуску отримуємо наступний результат:



“5431386178”

При повторному запуску результат не зміниться

Якщо ми змінемо строку “Random random = new Random(1234567890);” на “Random random = new Random(2023);” отримаємо наступний результат:



“6484653433”

Послідовність чисел змінилася.

Висновок: Результат отриманий через клас Random функцією Next буде відрізнятися лише при зміні початкового значення параметру “зерна”.

**Завдання 4:**

Написати програму, яка забезпечує генерацію та виведення на екран криптографічно стійкої послідовності випадкових чисел. Порівняти елементи послідовності для декількох послідовних спроб. Зробити висновки.

Код програми:

using System.Security.Cryptography;

namespace Lz1\_2

{

internal class Program

{

static void Main(string[] args)

{

var rndNumberGenerator = new RNGCryptoServiceProvider();

var randomNumber = new byte[9];

rndNumberGenerator.GetBytes(randomNumber);

var ConvertedResult = Convert.ToBase64String(randomNumber);

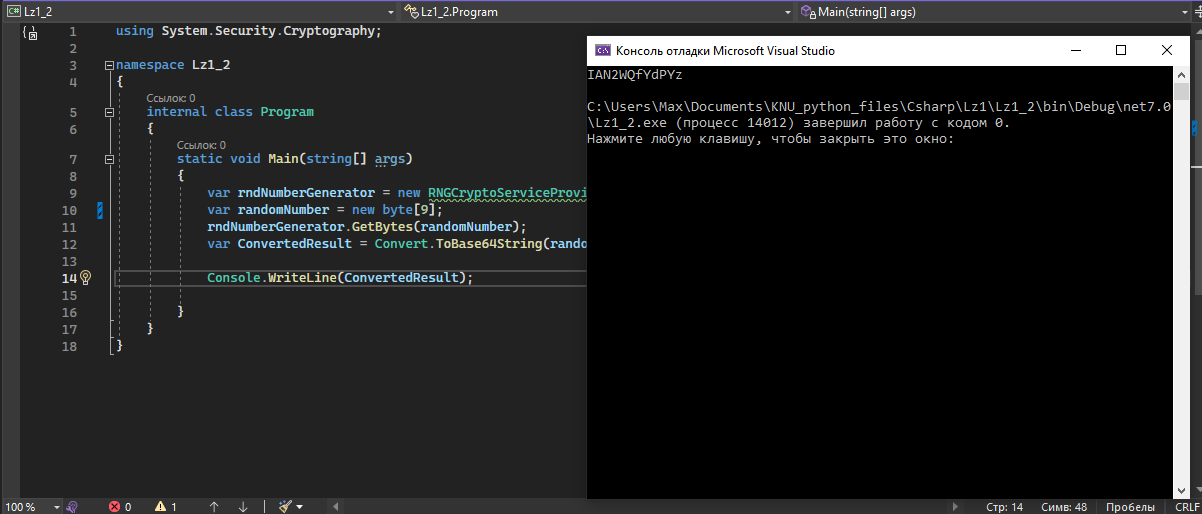
Console.WriteLine(ConvertedResult);

}

}

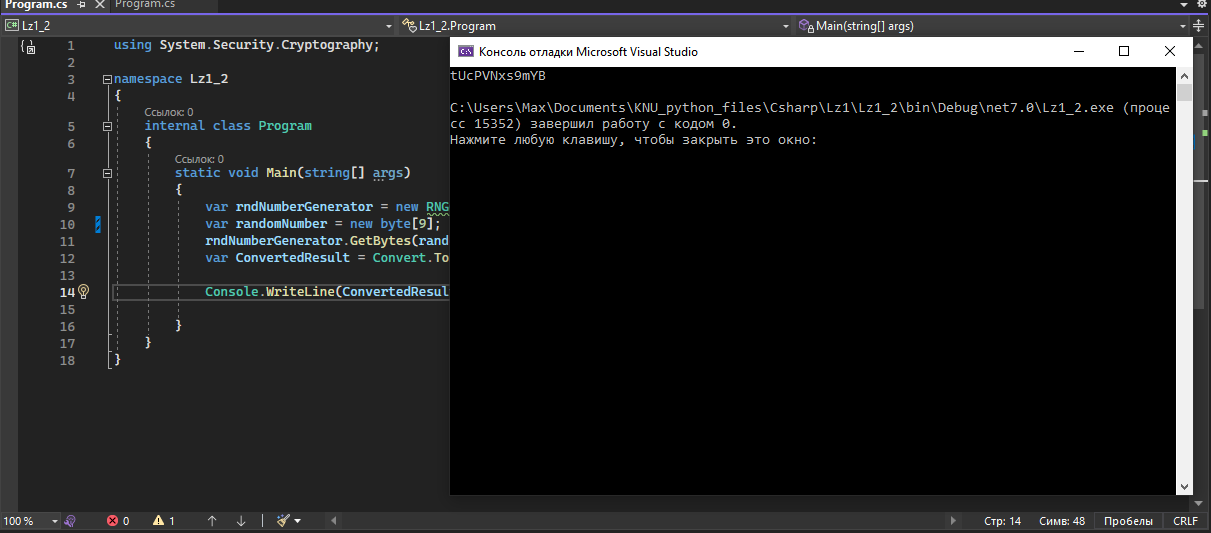
}

Результат запуску №1:



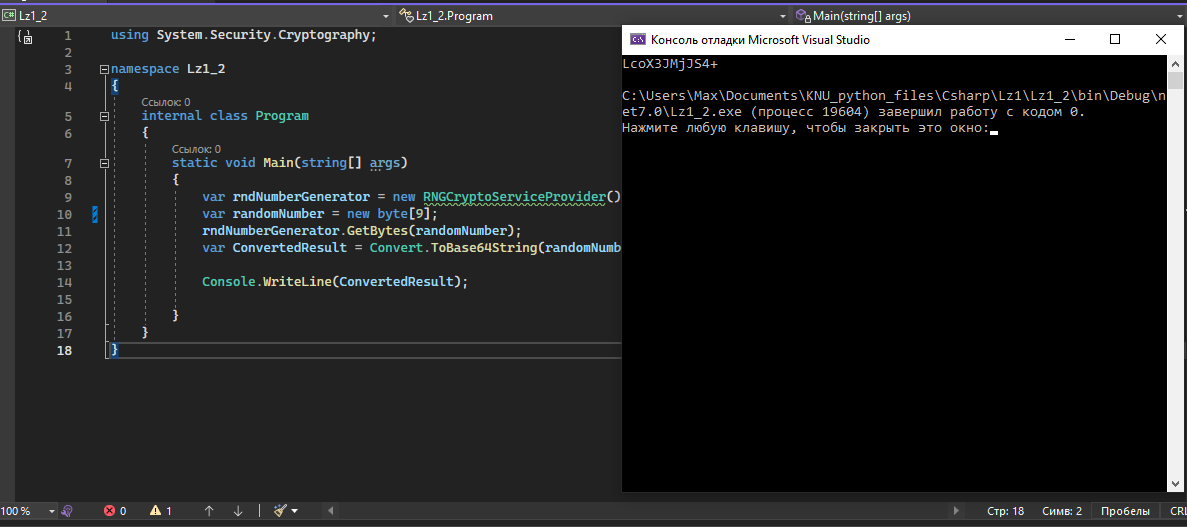
“IAN2WQfYdPYz”

Результат запуску №2:



“tUcPVNxs9mYB”

Результат запуску №3:



“LcoX3JMjJS4+”

Висновок: Функція GetBytes класу RNGCryptoServiceProvider повертатиме нові значення кожного разу, а також не вимагає початкового значення “зерна”, а тому є безпечнішою для генерування ключів за попередньо розглянуту функцію.

Посилання на репозиторій GitHub: https://github.com/MaxDashk3/Fundamentals-of-information-security-labs