Звіт з Основ інформаційної безпеки №1

Лончук Павло МІТ-21

1 - Генерація псевдовипадкових чисел

1) Підключаємо простір імен System



2) Cтворюємо клас під назвою Prog\_rnd і створимо свій метод, який повинен називатися Main.



3) Для генерації випадкових чисел нам треба використати клас Random, який базується на seed значенні. Дамо користувачу можливість вказувати seed, кількість чисел, їх максимальні та мінімальні значення. Залежно від його значення ми будемо мати різні результати програми.



4) Також створимо функцію яка мінятиме місцями значення min і max якщо max менше ніж min.



5) Ініціюємо генератор певним початковим значенням за допомогою оператора new. Для генерації послідовності ми створюємо цикл for, який буде виконуватись n разів і виводити псевдо випадкові числа. За допомогою методу Next() ми отримаємо наші псевдо випадкові числа. Для того, щоб задати діапазон бажаних псевдо випадкових чисел, у дужках методу Next() записуємо 2 числа через кому, в межах яких будуть наші числа. В нашому випадку ці значення вводить користувач. А також зробимо так щоб наші числа виводились через кому.





2 - Генерація криптографічно стійкої послідовності випадкових чисел

1) Для того, щоб наша послідовність була зашифрована нам треба використати метод RandomNumberGenerator.Create. Підключаємо простір імен System.Security.Cryptography. Потім створюємо свій клас Rand\_Crypto і метод Main.

2) Спочатку створюємо метод GenerateRandNum(), який міститиме в собі масив байтів. У цьому методі створюємо об’єкт методу RandomNumberGenerator.Create(). Створюємо сам масив байтів, числа якого будуть за довжиною заданим певним числом. Далі викличемо метод GetBytes і передамо в нього створений масив.



3) Далі просто створюємо цикл для виводу нашої генерації, який буде виконуватись n разів. Створимо об’єкт, який буде викликати наш метод створення масиву байтів і відповідного значення випадкового числа. Значення n задає користувач.



4) Для конвертування массива байтів у рядок, викликаємо метод Convert.ToBase64String. Таким чином отримаємо читабельний результат програми.



