Міністерство освіти і науки

Київський національний університет імені Тараса Григоровича Шевченка

Кафедра Мережевих та Інтернет технологій

**Звіт**

з практичної роботи **№2**

з дисципліни: “Основи інформаційної безпеки”

**«Реалізація шифру Вернама»**

Виконав:

Студент групи МІТ-21

Горбун О. М.

**Результати виконання завдань роботи:**

За завданнями практичної роботи було створено програми, які можна переглянути за посиланням:

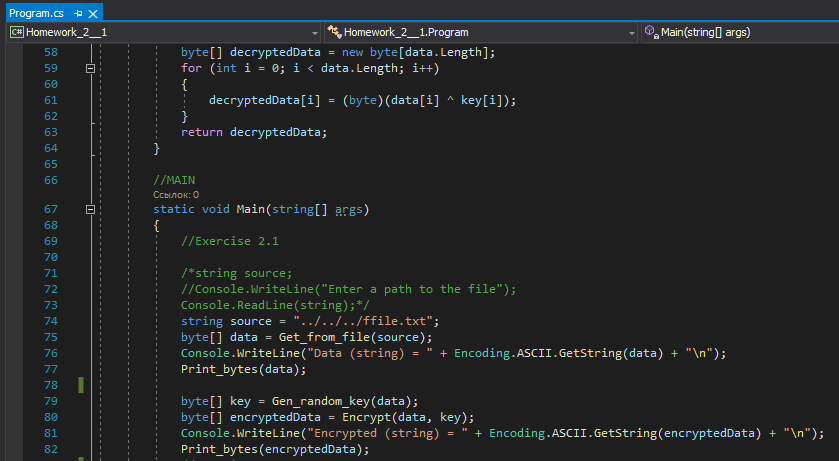
<https://github.com/OleksandrHorbun/Basics_Cybersecurity.git> (Посилання на відкритий репозиторій у веб-сервісі GitHub) завдання у вітці (Branch) Homework\_2.

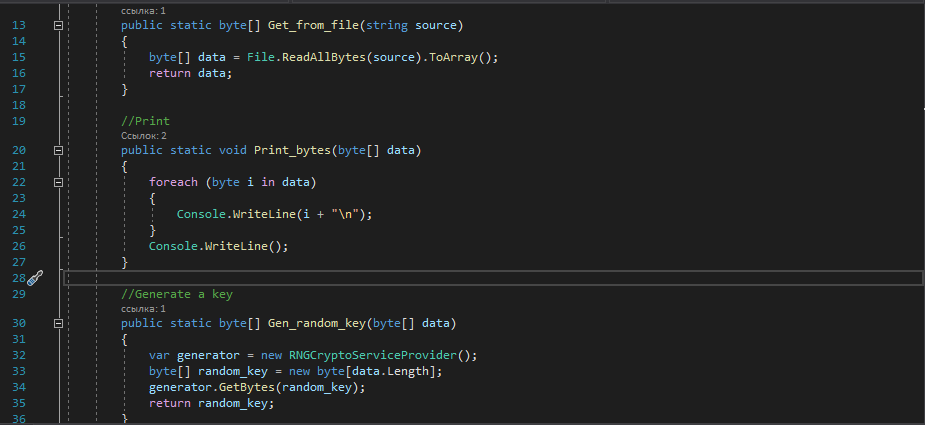
**I частина (перше завдання)**

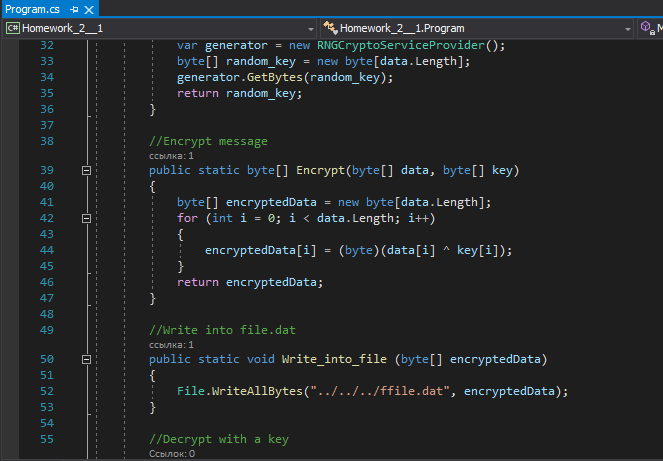
Як можемо побачити, спочатку програма отримує посилання на файл (у нашому випадку – «ffile.txt», який я створив та додав у папку проекту самостійно). Одразу після цього запускається функція *Get\_from\_file* (отримує шлях до файлу, записує у масив байтів текст з вищевказаного файлу та повертає у Main). Про всяк випадок я також виводжу на екран рядок з файлу. Далі іде функція *Print\_bytes* (Просто виводить по одному байту через рядок).

Наступним кроком починається процес шифрування, який також розподілений між функціями. Спочатку створюється масив випадкових ключів за допомогою функції *Get\_random\_key* (ініціалізується генератор рандомних криптографічних чисел, який наповнює випадковими числами попередньо створений порожній масив байтів. Отриманий результат повертається у Main). Основна частина шифрування за допомогою шифру Вернама відбувається у функції *Encrypt* (для кожного байту з масиву даних, зчитаних з файлу та байту з масиву ключів відбувається операція XOR (виключне АБО), результат записується по-елементно (по байту) записується у новий масив, повертається у Main). Одержаний масив зашифрованої інформації теж, про всяк випадок, виводиться на екран, як звичайний рядок і як послідовність байтів (за допомогою функції *Print\_bytes*). Крім цього результат ще записується у файл «ffile.dat» за допомогою функції *Write\_into\_file*.

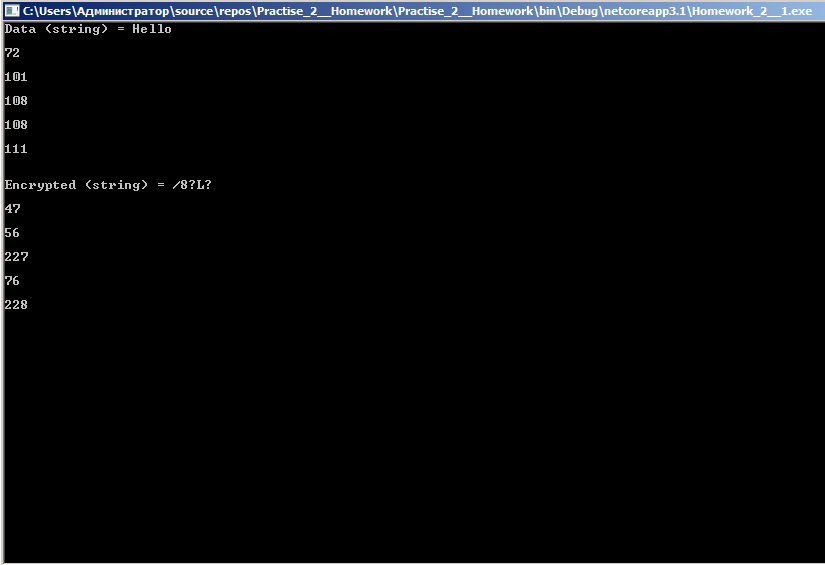
Все описане вище можна побачити на знімках екрану:







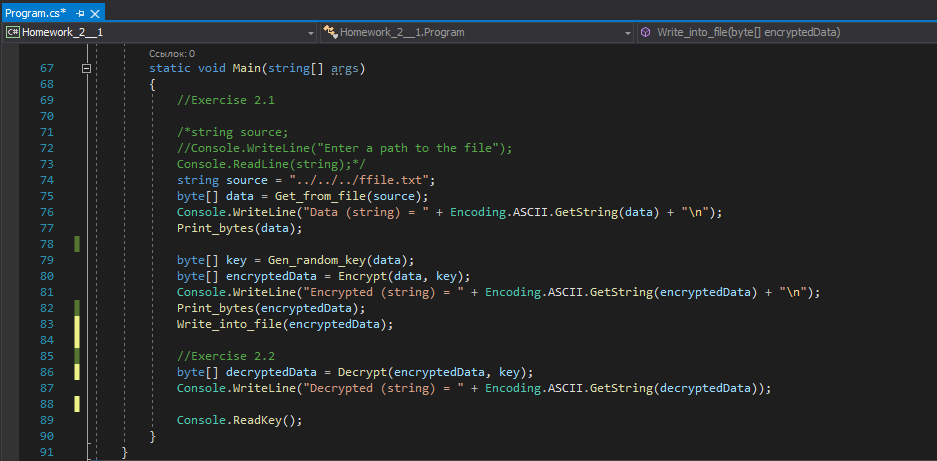


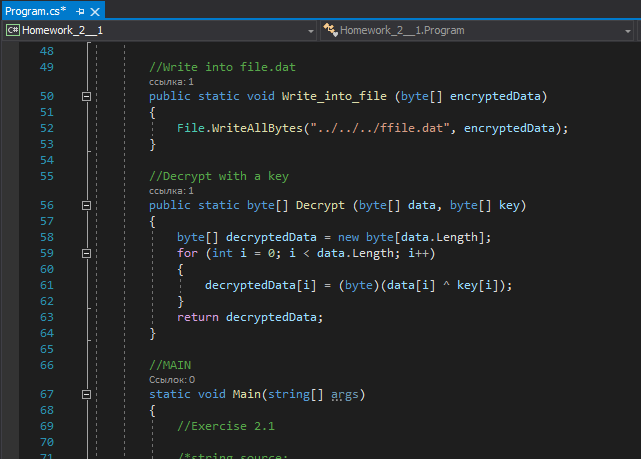


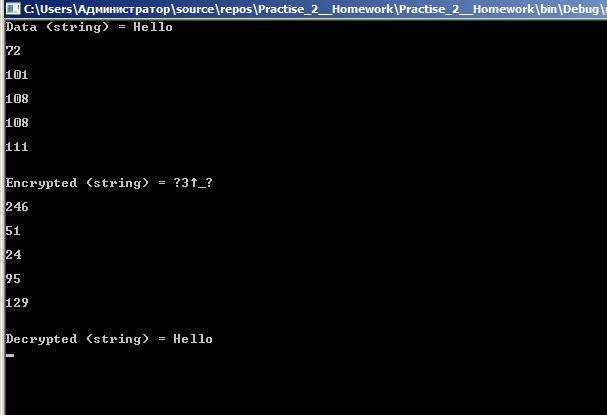
**IІ частина (друге завдання)**

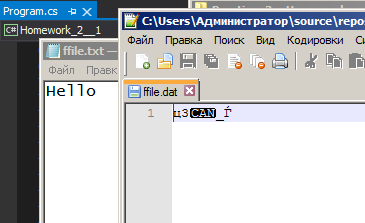
У програмі друга частина є продовженням першої (під час демонстрації першої була закоментована). Для реалізації була створена функція *Decrypt* (приймає вже зашифровані дані, для кожного елементу (байту) з масиву зашифрованих даних і байту з масиву ключів знову проводить операцію XOR (виключне АБО). Тобто, фактично навпаки – з зашифрованих елементів таким чином одержуються розшифровані дані, які записуються у новий масив, повертається у Main). У кінці розшифровані дані виводяться рядком користувачу на екран, що дає змогу точно перевірити роботоспроможність програми.

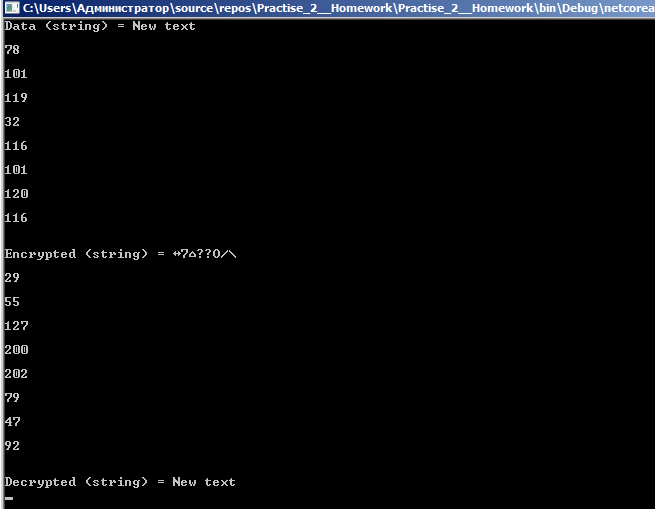
Все описане вище (разом ще раз з попереднім завданням) можна побачити на знімках екрану:











**Висновок:**

Виконуючи цю роботу я навчився створювати програми для зчитування, шифрування, розшифрування, запису даних, зрозумів як реалізовувати шифр Вернама за допомогою мови програмування C# і тепер знаю як користуватись вивченим у цій практичній матеріалом на практиці.