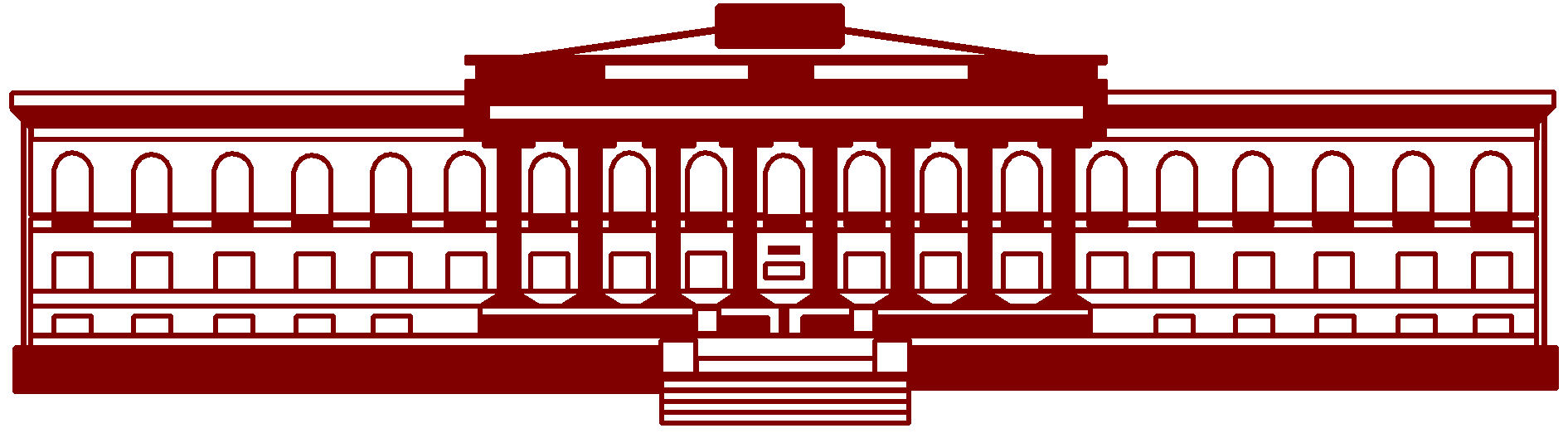
**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**імені ТАРАСА ШЕВЧЕНКА**

****

**ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**Кафедра прикладних інформаційних систем**

**Звіт до лабораторної роботи №8**

**З курсу**

**«Безпека мереж і комп’ютерних систем»**

*студента 2 курсу*

*групи ПП-22*

*спеціальності 122 «Комп'ютерні науки»*

*ОП «Прикладне програмування»*

Шевлюк Вікторії Віталіївни

*Перевірив:*

д.т.н, професор

Сайко В. Г.

**Київ 2022**

**Тема:** Односпрямовані хеш-функції.

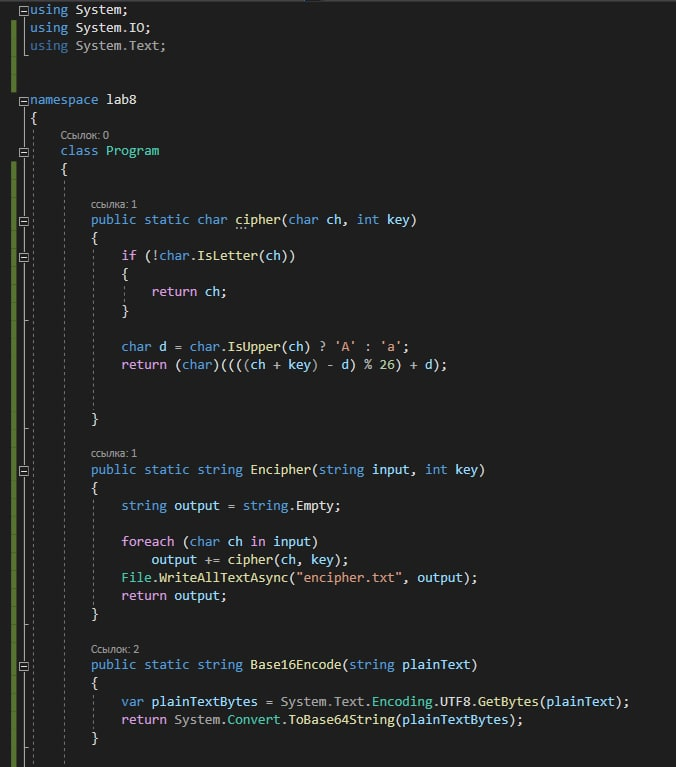
**Мета:** Ознайомитися з різними алгоритмами формування хеш-функцій. Вивчити їх сфери застосування та основні властивості. Розглянути класи атак, спрямованих на аналіз хеш-функцій. Розглянути прості хеш-функції.

**Завдання:**

1. Вивчити основні теоретичні положення стосовно використання і формування односпрямованих хеш-функциій.
2. Реалізувати програмно просту функцію хешування, основану на використанні операції XOR із застосуванням рандомізації:
   * початкове повідомлення *М* береться з текстового файлу "text.txt";
   * розрядність хеша вибрати рівною 16-ти бітам;
   * значення хеш-функції зберегти у файлі "hash.txt".

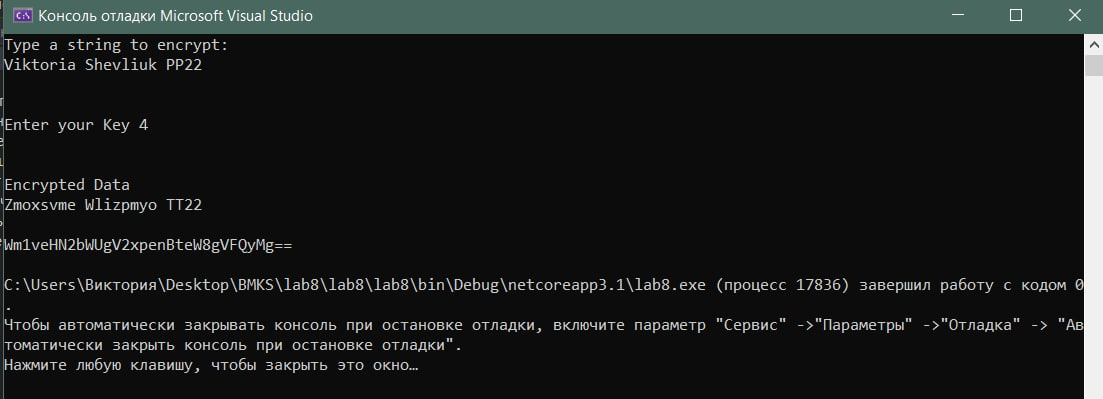
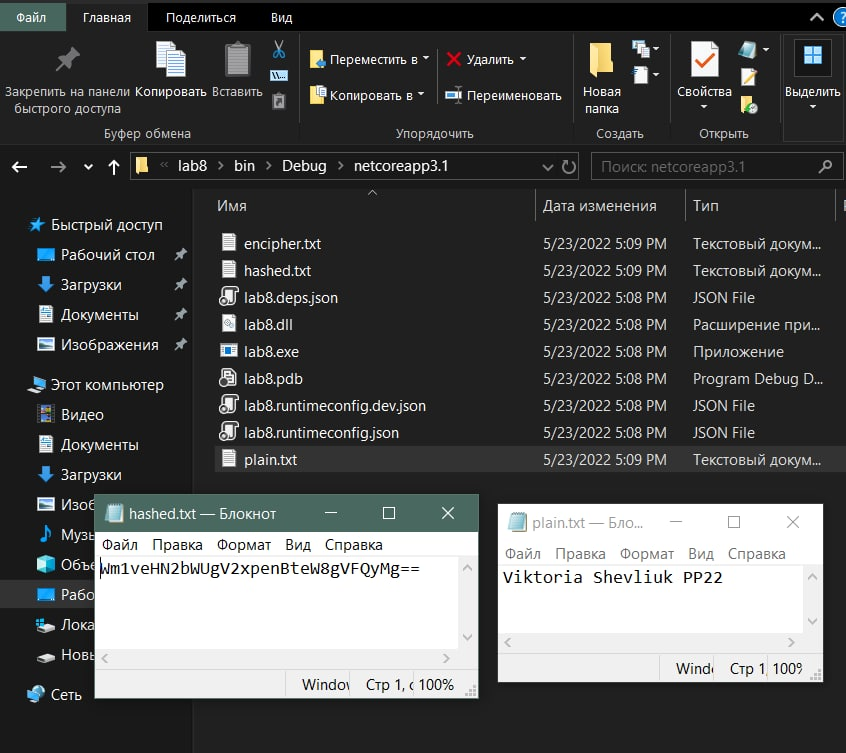
**Хід роботи:**

Створимо мовою С# програму, що буде реалізовувати функцію хешування, засновану на операції Ксор та рандомізацї.

Ось так виглядає код програми:



Результат роботи програми:



**Висновок:** у ході даної лабораторної роботи я ознайомилася з різними алгоритмами формування хеш-функцій та простими хеш-функціями. Хеш-функція— [функція](https://uk.wikipedia.org/wiki/%D0%9F%D1%96%D0%B4%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0), що перетворює вхідні дані будь-якого (як правило великого) розміру в дані фіксованого розміру. Хешування— перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини. Такі перетворення також називаються хеш-функціями, або функціями згортання, а їхні результати називають хешем, хеш-кодом, хеш-сумою, або дайджестом повідомлення Хеш-функція використовується зокрема у структурах даних — [хеш-таблицях](https://uk.wikipedia.org/wiki/%D0%A5%D0%B5%D1%88-%D1%82%D0%B0%D0%B1%D0%BB%D0%B8%D1%86%D1%8F), широко вживаних у програмному забезпеченні для швидкого пошуку даних. Хеш-функції використовуються для оптимізації таблиць та баз даних користуючись з того, що в однакових записів однакові значення хеш-функції.

**Контрольні питання:**

1. ***Що таке хеш-функція? Для чого вона призначена?***

[Функція](https://uk.wikipedia.org/wiki/%D0%9F%D1%96%D0%B4%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0), що перетворює вхідні дані будь-якого (як правило великого) розміру в дані фіксованого розміру.

1. ***Яки вимоги висуваються до хеш-функцій?***

Швидкість обчислення, мінімізація колізій

1. ***Що таке односпямованість?***

Односпрямована функція - це F(x), де:

Існує поліноміальний алгоритм для обчислення F(x), але не існує поліноміального алгоритму для інвертування F(x) = y

1. ***Що таке сильна та слабка стійкість до колізій?***

Хеш функція – це деяка функція h(K), яка бере ключ K і повертає адресу, по якому проводиться пошук в хеш-таблиці, щоб отримати інформацію, пов'язану з K. Колізія — це ситуація, коли h(K1) = h(K2)

1. ***Опишіть принцип формування хеш-коду зо допомогою операції ХOR. В чому недолік та перваги цього підходу?***

На вхід функція отримує слово W  що складається з n символів, кожен розміром 1 байт, і повертає значення в діапазоні від 0 до 255. При цьому значення геш-коду залежить від кожного символу вхідного слова.

Алгоритм можна описати таким псевдокодом, який отримує на вхід рядок W та використовує таблицю перестановок Т.

Переваги - простота обчислення; не існує таких вхідних даних, для яких імовірність колізії найбільша; можливість модифікації в ідеальну геш-функцію, але вона неефективна для захисту даних, коли з відкритим повідомленням передається шифрований хеш-код. Маючи деяке повідомлення, зовсім неважко створити нове повідомлення, якому відповідатиме той же самий хеш-код: просто підготуйте будь-яке необхідне альтернативне повідомлення і приєднаєте до нього відповідний -бітовий блок, який разом з новим повідомленням сформує бажаний хеш-код.

1. ***Опишіть алгоритм формування хеш-коду з використанням операції ХOR з ефектом рандомізації.***

Початкова ініціалізація -бітового значення функції хешування нульовим значенням. Послідовна обробка -бітових блоків даних за наступним правилом:

► виконання циклічного зсуву поточного значення функції хешування вліво на один біт;

► додавання поточного блоку до значення функції хешування з допомогою операції XOR.