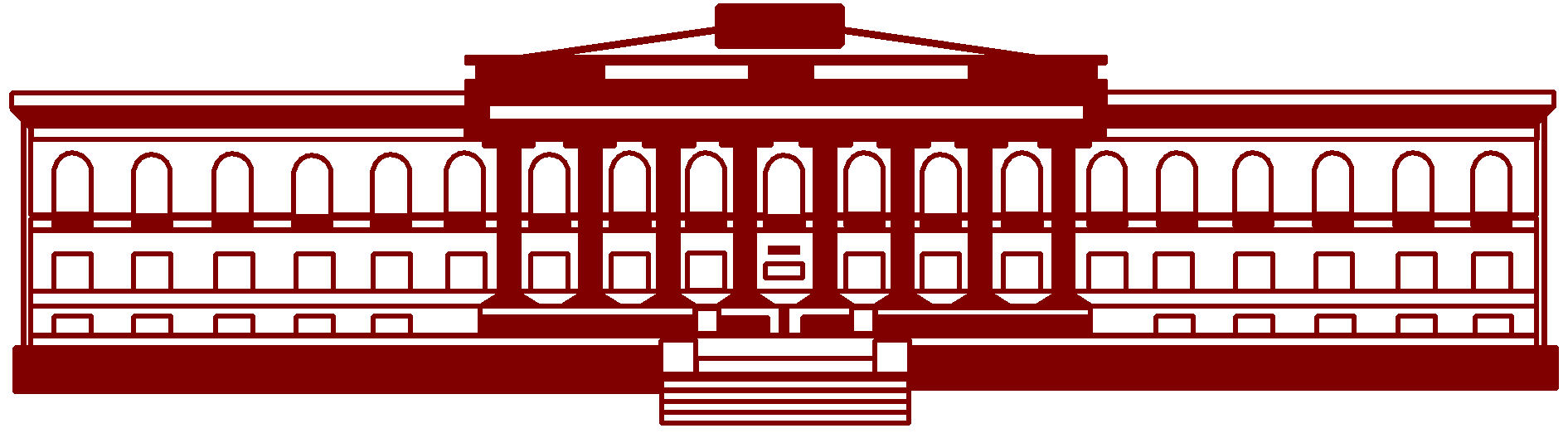
**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**імені ТАРАСА ШЕВЧЕНКА**

****

**ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**Кафедра прикладних інформаційних систем**

**Звіт до лабораторної роботи №10**

**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:** Блокові симетричні алгоритми шифрування

**Мета:** Ознайомитися з основними поняттями, присвяченими принципам функціонування блокових алгоритмів. Дослідити структуру шифру Фейстеля.

**Завдання:**

1. Вивчити основні теоретичні положення стосовно блокових криптоалгоритмів.
2. Реалізувати програмно блоковий шифр, заснований на шифрі Фейстеля:
   * відкритий текст отримується з текстового файлу "open.txt". Розмір блоку вхідних даних для шифрування дорівнює  біт;
   * ключ задається в тілі програми. Розмір ключа складає *N* біт;
   * число раундів обробки дорівнює ;
   * шифротекст виводиться на екран.

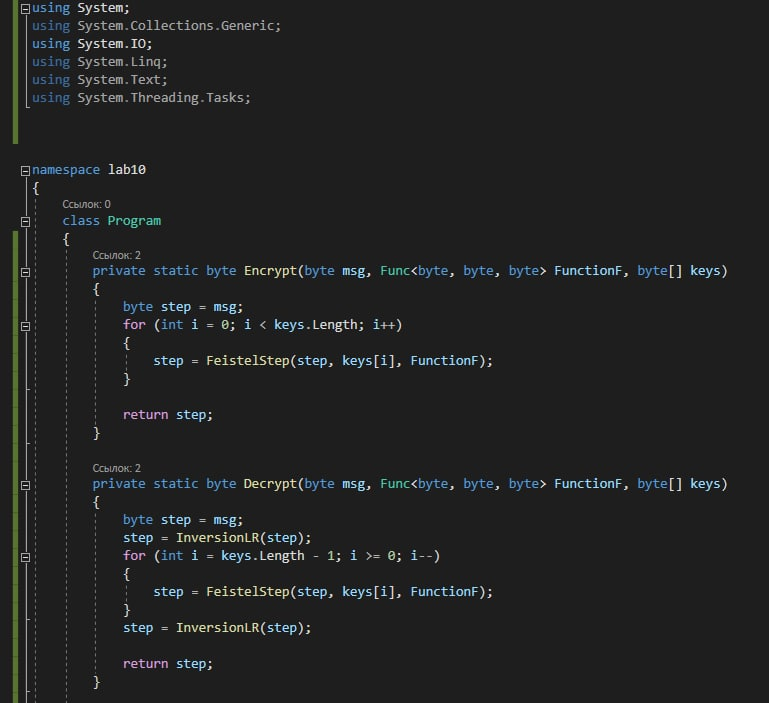
Параметри , а також алгоритм обчислення підключів і функція раунду вибираються згідно з варіантом, виданим викладачем.

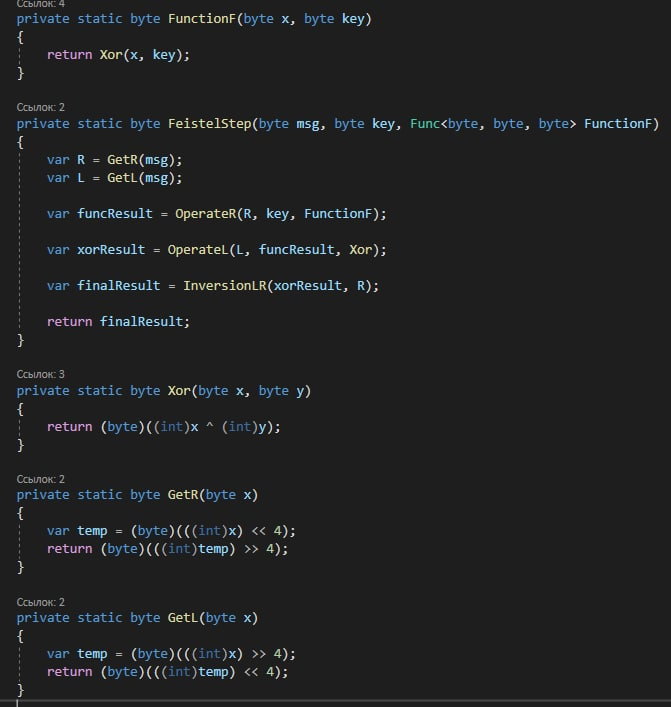
**Хід роботи:**

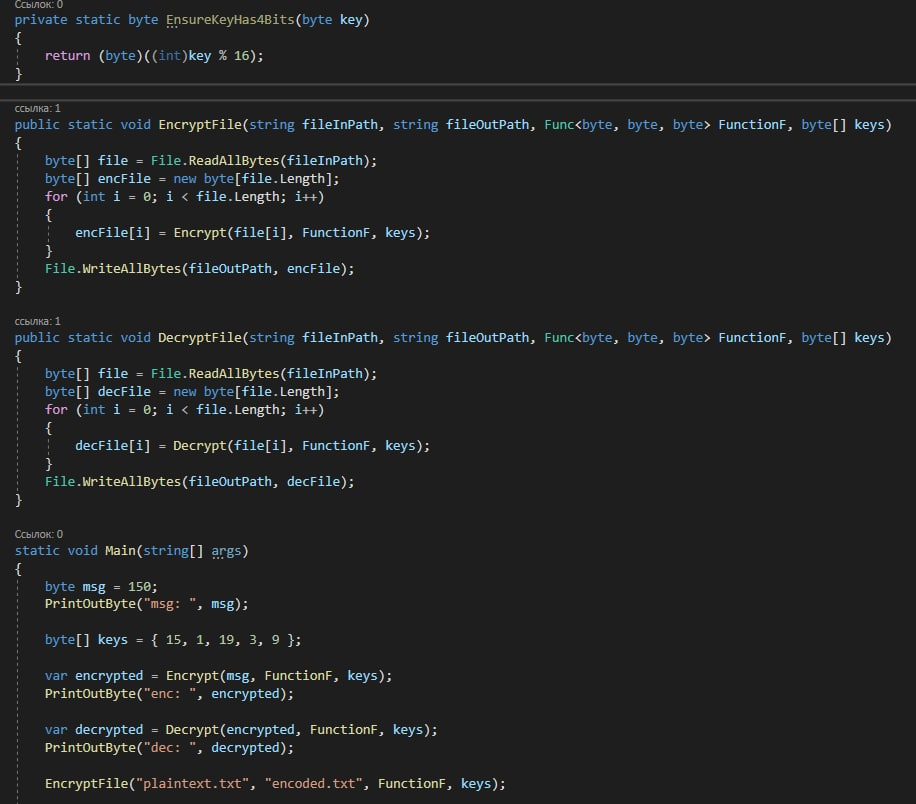
Напишемо мовою С# програму, що буде реалізовувати шифр Фейстеля, що буде працювати наступним чином:

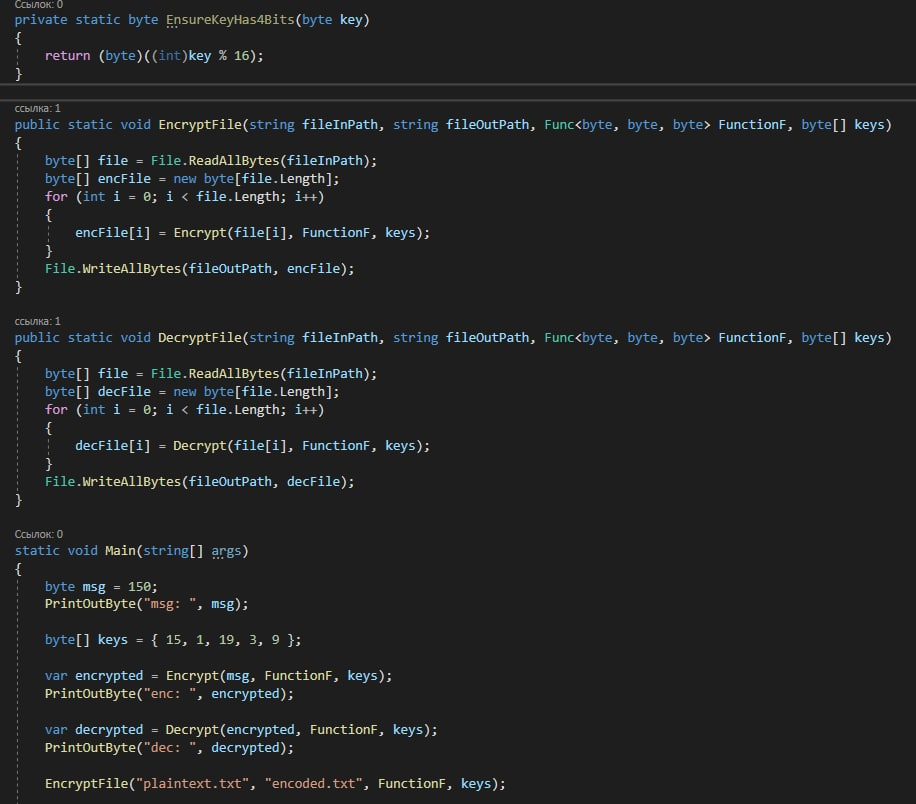
відкритий текст отримується з текстового файлу "open.txt". Розмір блоку вхідних даних для шифрування дорівнює  біт; ключ задається в тілі програми. Розмір ключа складає *N* біт; число раундів обробки дорівнює ; шифротекст виводиться на екран.

Нижче наведений код моєї програми:

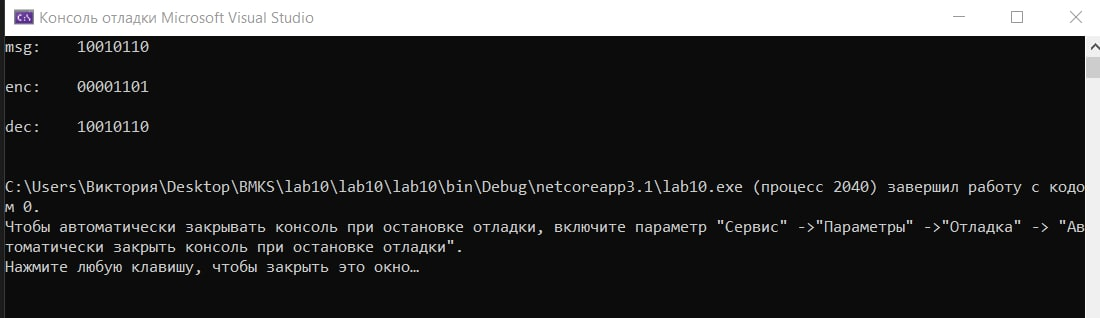


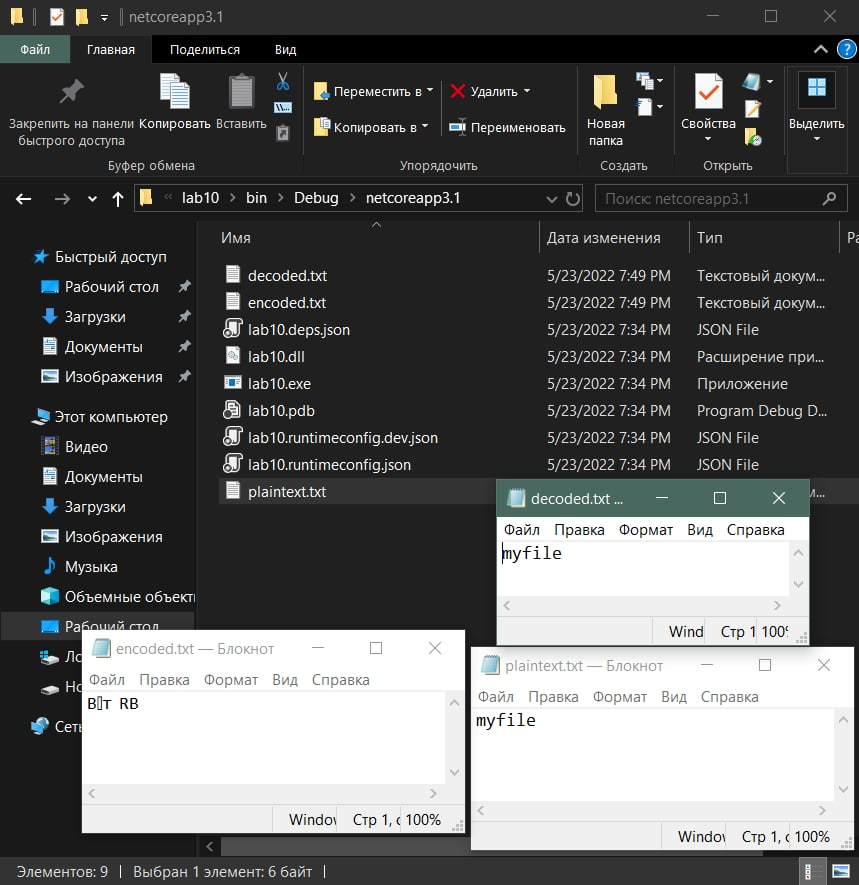






Результат роботи програми:





**Висновок:** під час цієї лабораторної роботи я ознайомилася з основними поняттями, присвяченими принципам функціонування блокових алгоритмів і дослідила структуру шифру Фейстеля. **Мережа Файстеля** (конструкція Файстеля) — різновид [блочного шифру](https://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D1%87%D0%BD%D1%96_%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%D0%B8_%D1%88%D0%B8%D1%84%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F) з певною ітеративною структурою. Багато сучасних алгоритмів використовують мережу Файстеля як основу.

**Контрольні питання:**

* 1. ***Які принципи блокового шифрування ви знаєте?***

Обробка блоку декількох байт за одну ітерацію (як правило 8 або 16)

* 1. ***У чому відмінність між блоковими і потоковими шифрами?***

Потоковий шифрує потік байтів, блочний шифрує блоки з декількох байтів за ітерацію

* 1. ***Які вимоги висуваються до функції шифрування для блокових шифрів?***

До функції блокового шифрування  висуваються наступні вимоги:

Функція  має бути зворотною.

Не повинно існувати інших методів отримання повідомлення  по відомому блоку , окрім як повним перебором ключів .

Не повинно існувати інших методів визначення, яким ключем було зашифроване повідомлення, окрім як повним перебором ключів

* 1. ***На чому заснована криптостійкість блокових шифрів?***

Щоб надати необхідну стійкість шифру, шифрувальна функція працює циклічно: це називається циклічним кодуванням

* 1. ***Які алгоритми блокового шифрування вам відомі?***

Ітераційні блочні шифри, SP-сітки, шифр Фейстеля

* 1. ***Опишіть структуру шифру Фейстеля.***

На вхід алгоритму шифрування подається блок відкритого тексту завдовжки  бітів і ключ . Блок відкритого тексту розділяється на дві рівні частини?,  й , які послідовно проходять через  раундів обробки, а потім об'єднуються знову для отримання блоку шифрованого тексту відповідної довжини.Для раунду  як вхідні дані виступають  и ,, отримані на виході поперднього раунду, і підключ , що обчислюється по загальному ключу . Усі підключі відрізняються як від загального ключа, так і один від одного. Усі раунди обробки проходять за однією і тією ж схемою. Спочатку для лівої половини блоку даних виконується операція підстановки. Вона полягає в застосуванні до правої половини блоку даних деякої функції раунду  і в наступному додаванні отриманого результату з лівою половиною блоку даних за допомогою операції ХОR. Для усіх раундів функція  має одну і ту ж структуру, але залежить від параметра – підключа раунда . Після підстановки виконується перестановка, дві половини блоку даних міняються місцями. Уся ця структура в цілому є частинним випадком так званої підстановлювально-перестановочної схеми, запропонованої Шеноном.Після закінчення останнього раунду виконується ще одна перестановка, яка, по суті, відміняє перестановку, виконану в останньому раунді. Тому, знехтувавши лише зовнішньою узгодженістю представлення, ці дві перестановки зі схеми можна видалити.

* 1. ***Дайте визначення поняттям дифузія і конфузія.***

Суть дифузії полягає в розсіянні статистичних особливостей відкритого тексту по широкому діапазону статистичних характеристик шифрованого тексту. Це досягається тим, що значення кожного елементу відкритого тексту впливає на значення багатьох елементів шифрованого тексту, або будь-який з елементів шифрованого тексту залежить від безлічі елементів відкритого тексту.

Що стосується конфузії, то перед нею ставиться завдання в максимальній мірі ускладнити статистичний взаємозв'язок між шифрованим текстом і ключем з метою протистояння спробам визначити ключ. Це досягається використанням складних підстановочних алгоритмів: прості лінійні подстановочні функції збільшують складність алгоритму лише в незначній мірі

* 1. ***Які параметри шифру Фейстеля вам відомі?***

Ключ, число раундів обробки, розмір вхідних даних та ключа