Звіт

До лабораторної роботи №6

З теми: «Забезпечення конфіденційності інформації з використанням симетричного шифрування»

Підготував

Студент групи МІТ-21

КНУ ім.Т.Г.Шевченка

Голомозик Кирило

1. Написати програму, яка виконує зашифровування та розшифровування

даних з використанням алгоритмів симетричного шифрування DES,

Triple-DES, AES. Секретний ключ та вектор ініціалізації генерується

випадковим чином.

2. Для програми з п.1. реалізувати можливість задання секретного ключа

та вектора ініціалізації за допомогою псевдовипадкової послідовності

із використанням пароля. «Сіль» генерувати як випадкову

послідовність байтів. Число ітерацій = номер варіанта \* 10'000.

Підказка: використовувати клас Rfc2898DeriveBytes)

Варіант 8.

**Завдання 1**

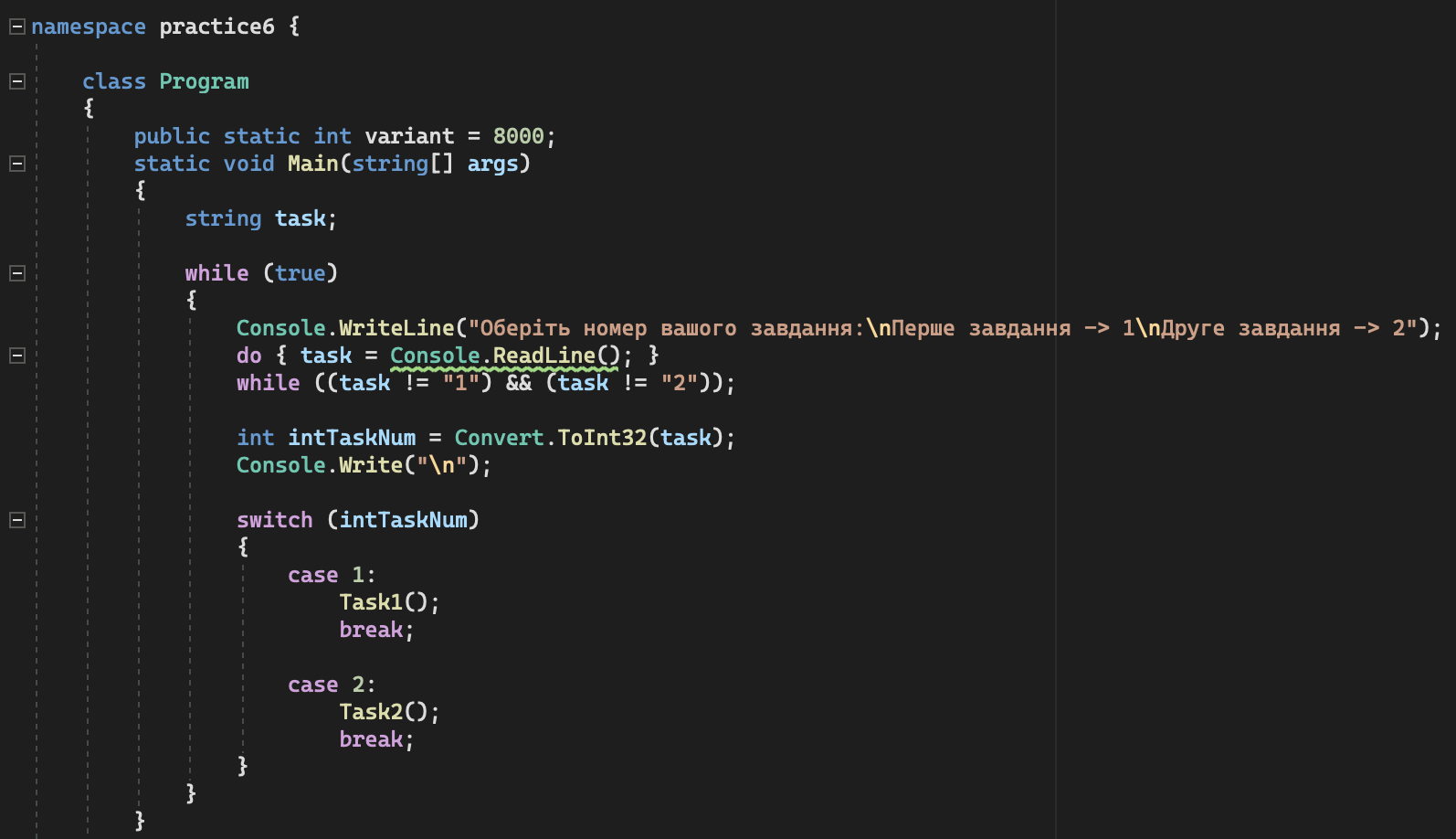
. Написати програму, яка виконує зашифровування та розшифровування

даних з використанням алгоритмів симетричного шифрування DES,

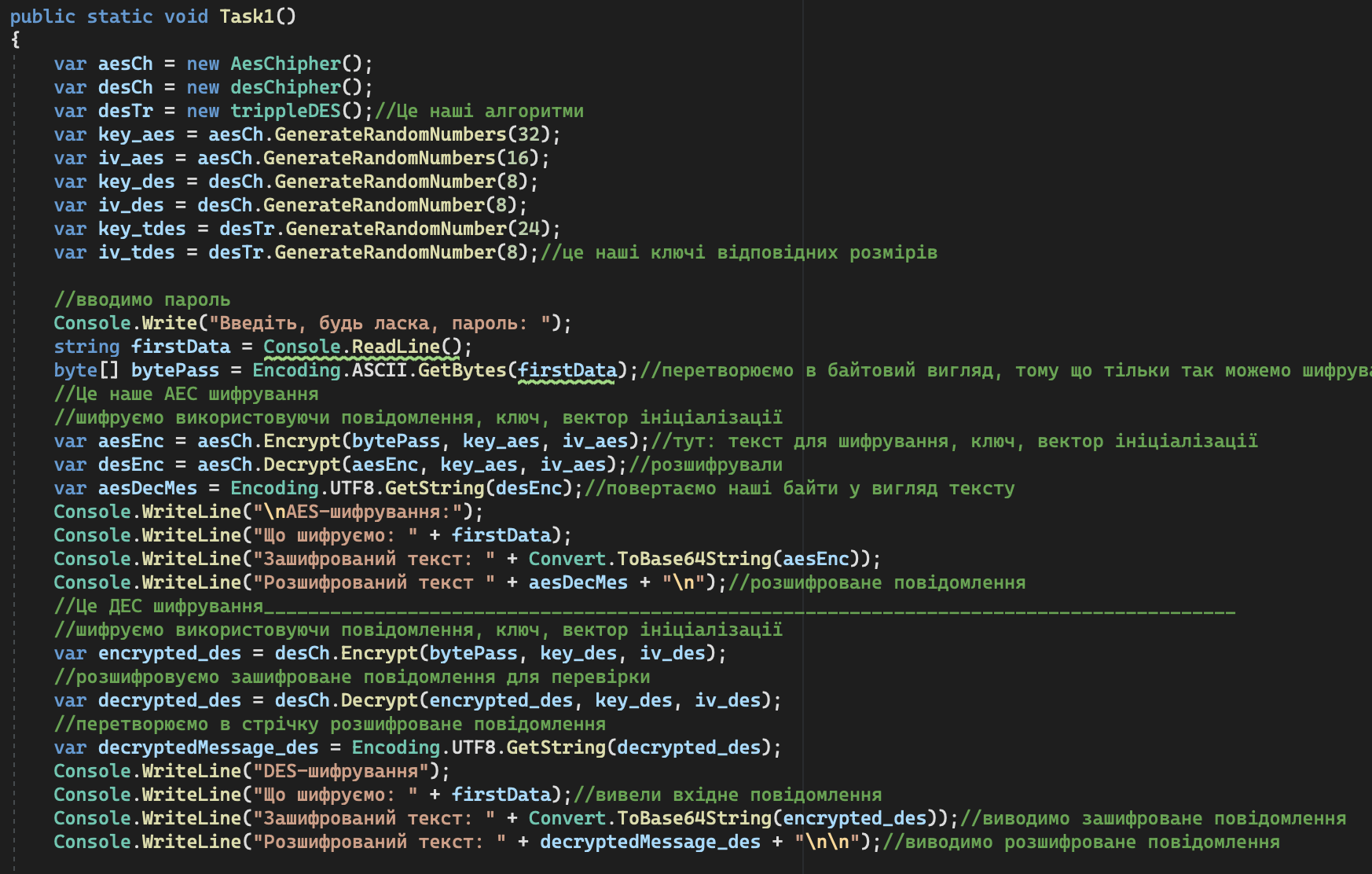
Triple-DES, AES. Секретний ключ та вектор ініціалізації генерується

випадковим чином.

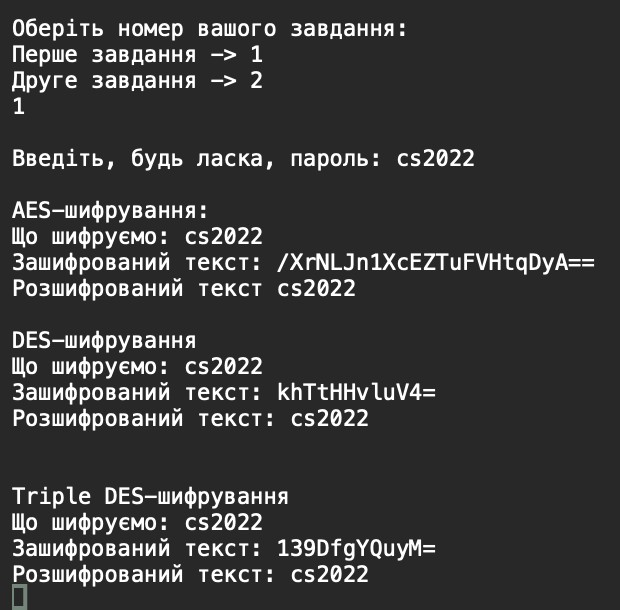
Зробив меню, як зазвичай, в якому можна вибрати завдання



Далі перше завдання



Працює так:



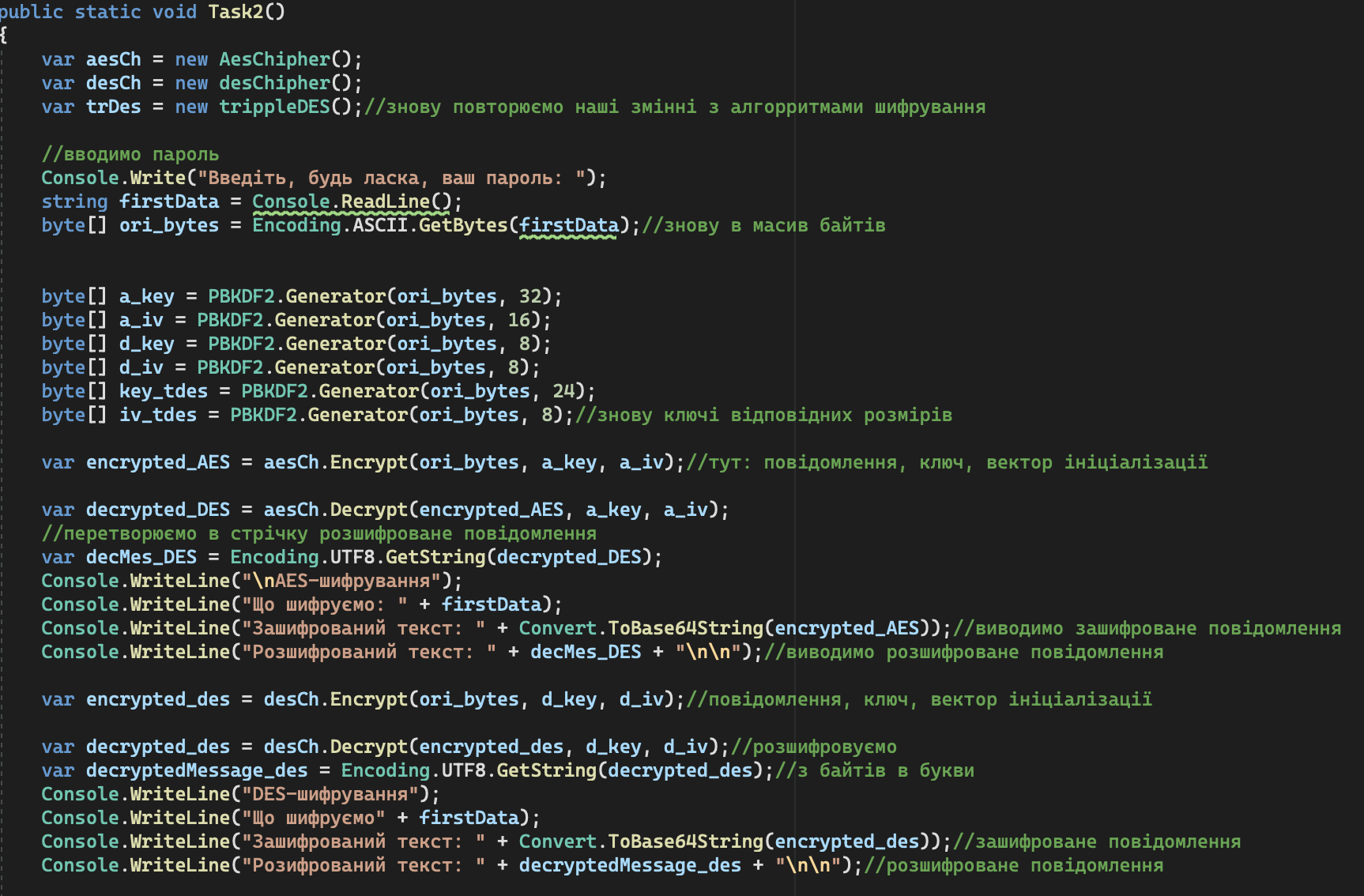
2. Для програми з п.1. реалізувати можливість задання секретного ключа

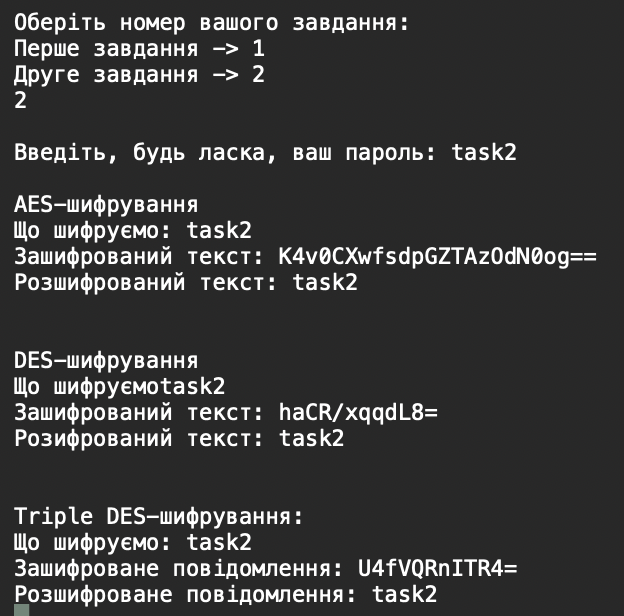
та вектора ініціалізації за допомогою псевдовипадкової послідовності

із використанням пароля. «Сіль» генерувати як випадкову

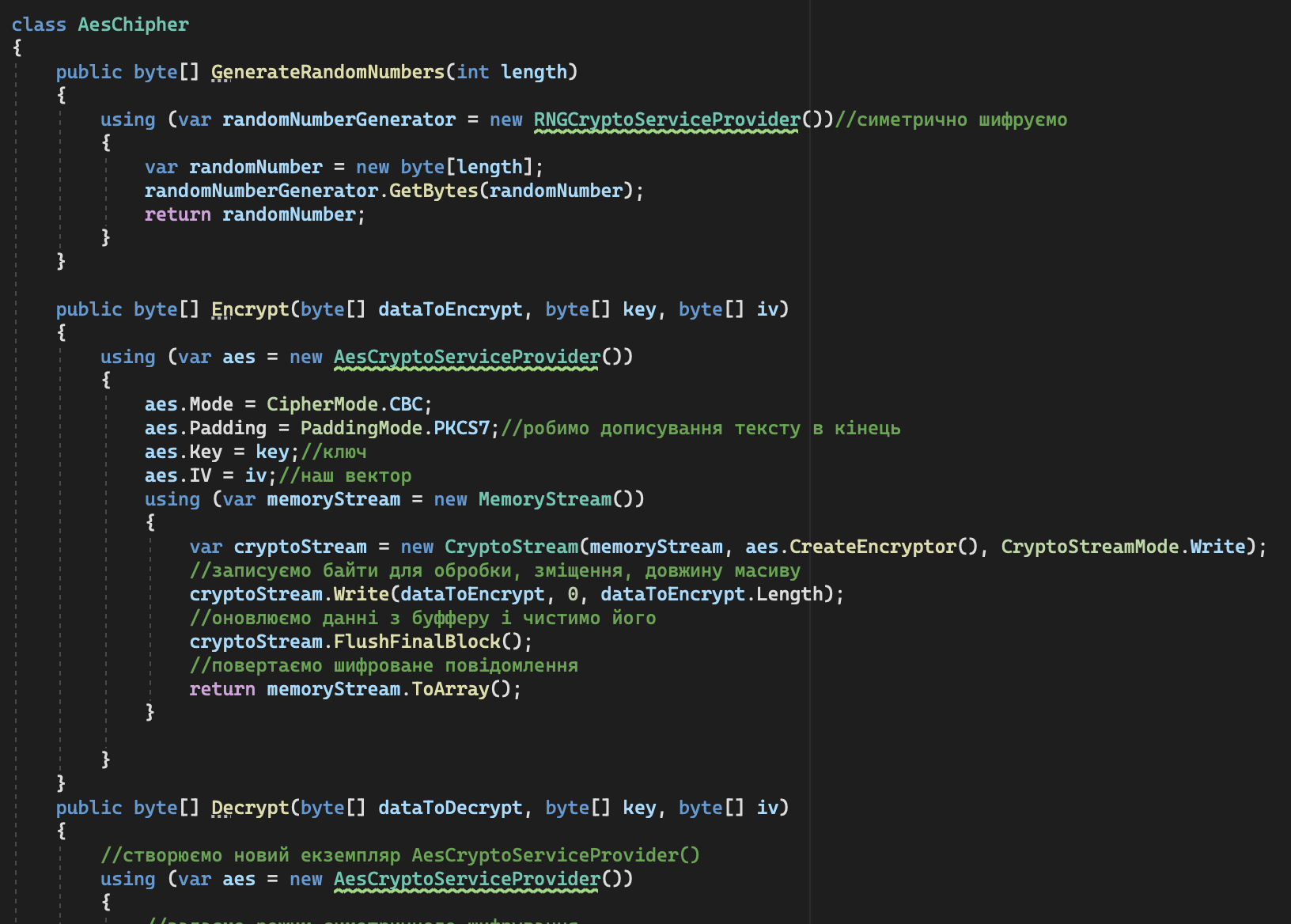
послідовність байтів. Число ітерацій = номер варіанта \* 10'000.

Підказка: використовувати клас Rfc2898DeriveBytes)





В Task1 та Task2 звертаюсь до классів, вони описані в нижній частині коду



**Висновок**: було на практиці розглянуто забезпечення конфіденційності інформації з використанням симетричного шифрування.