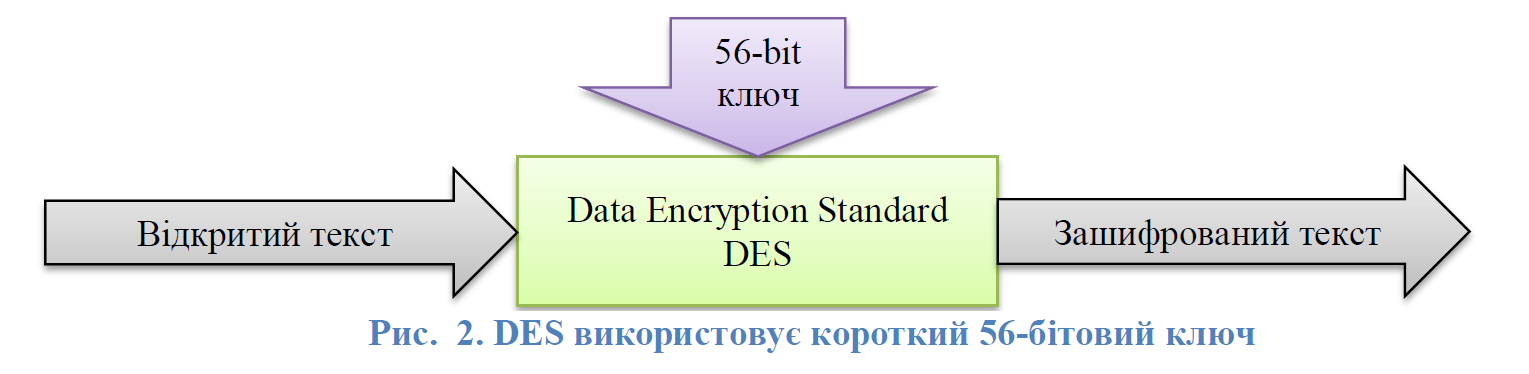
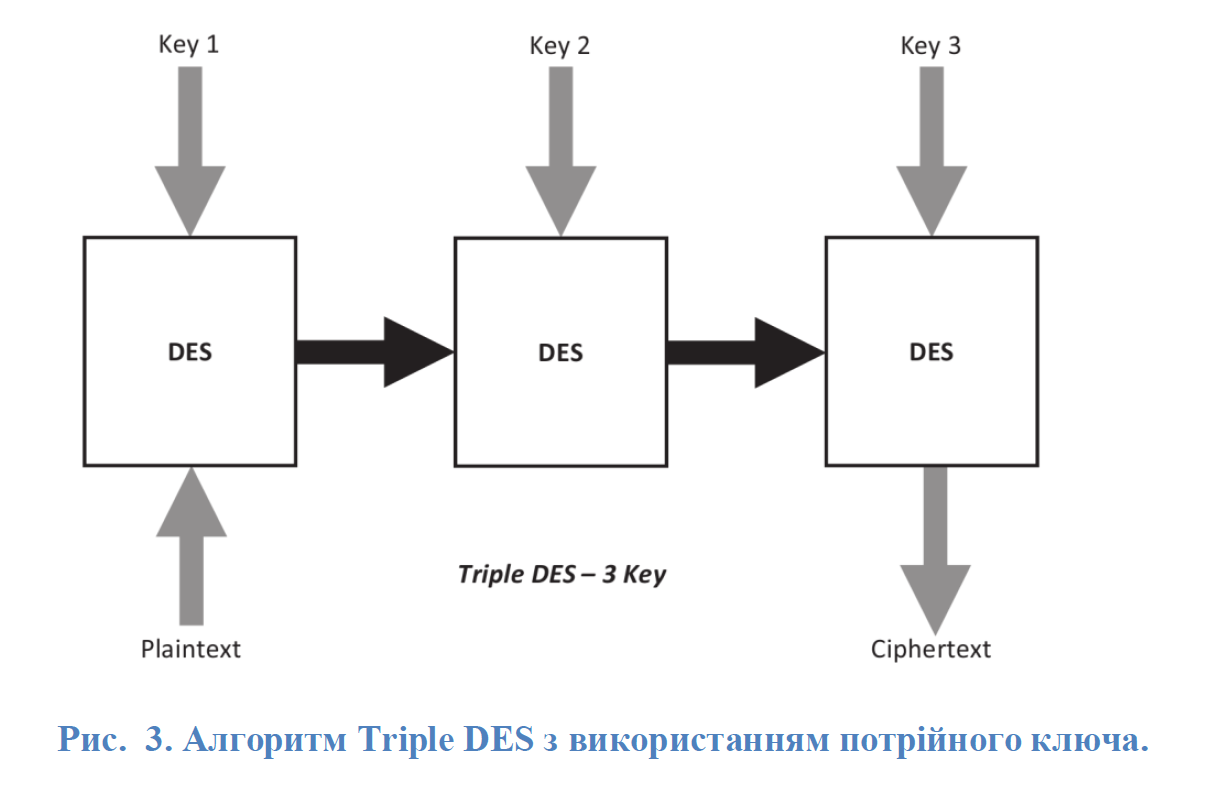
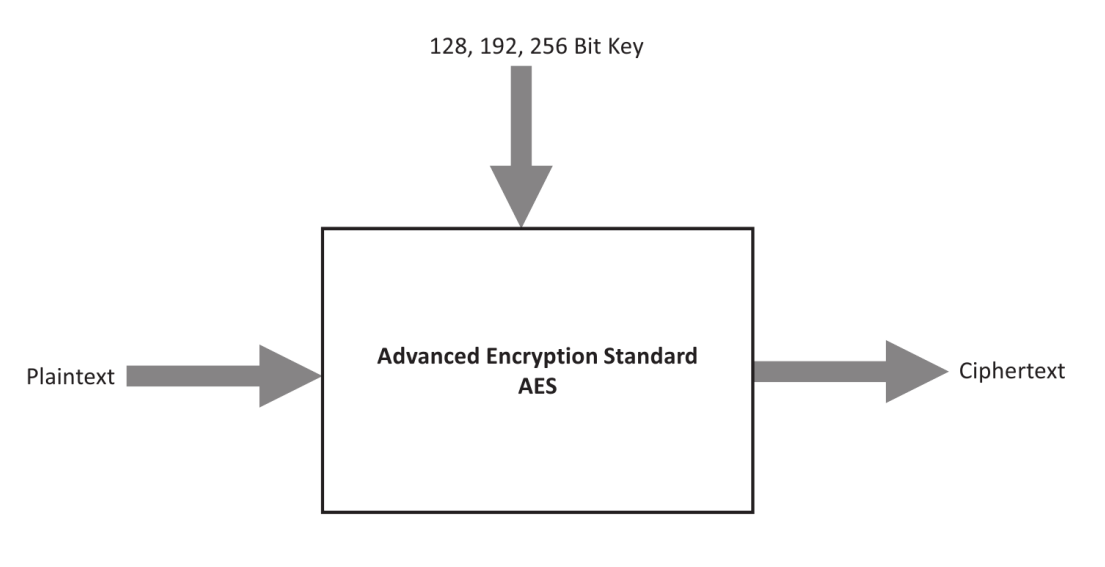
Звіт ПЗ\_6

МІТ-21 Квартюк Олексій

Тема: **«Забезпечення конфіденційності інформації з використанням симетричного шифрування»**







Переваги симетричного шифрування:

1) Швидкий

2) Надійній(AES взагалі є не зламною і рекомендованою на даний момент

Недоліки:

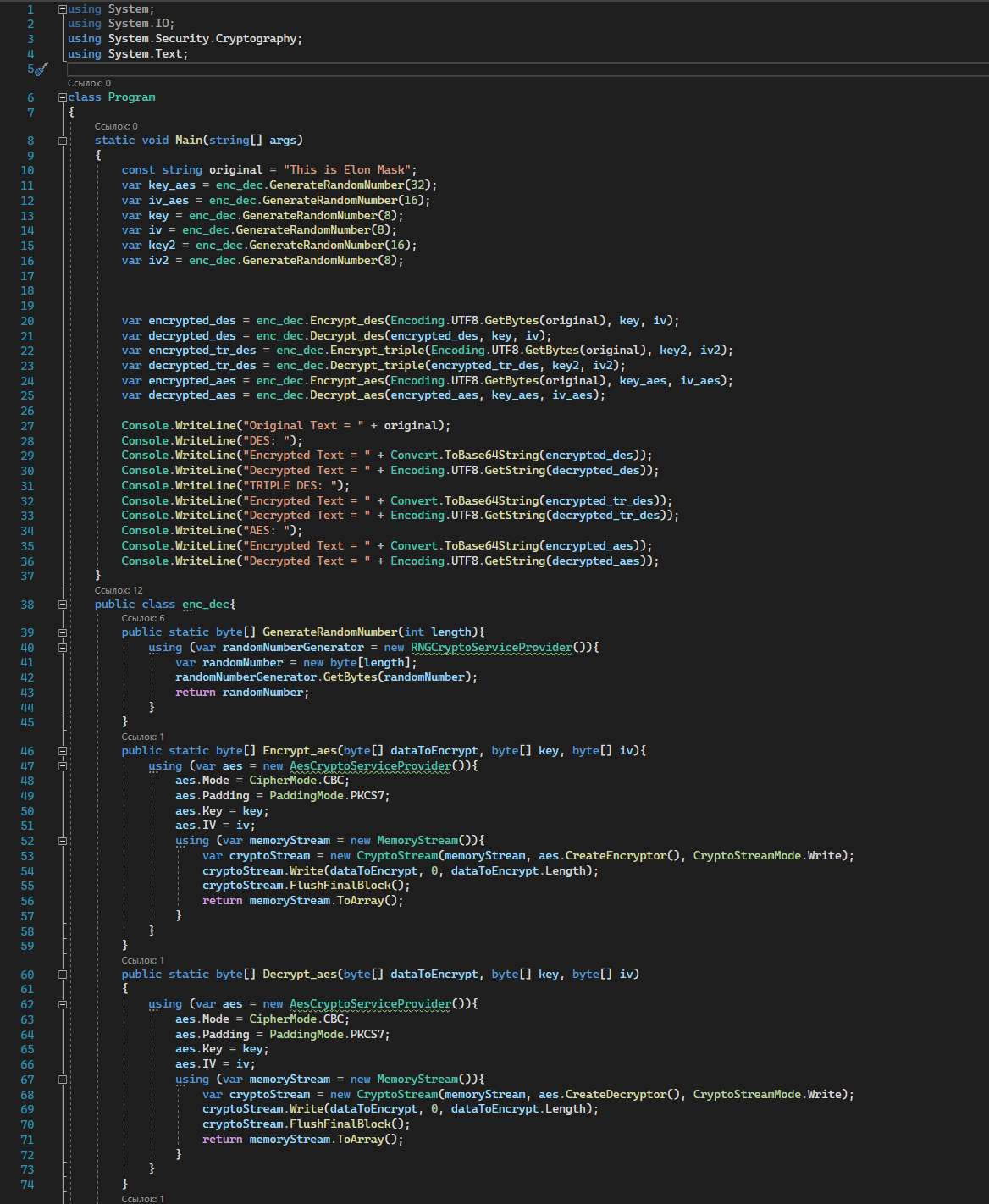
1) Потрібно надавати відкритий ключ іншим особам

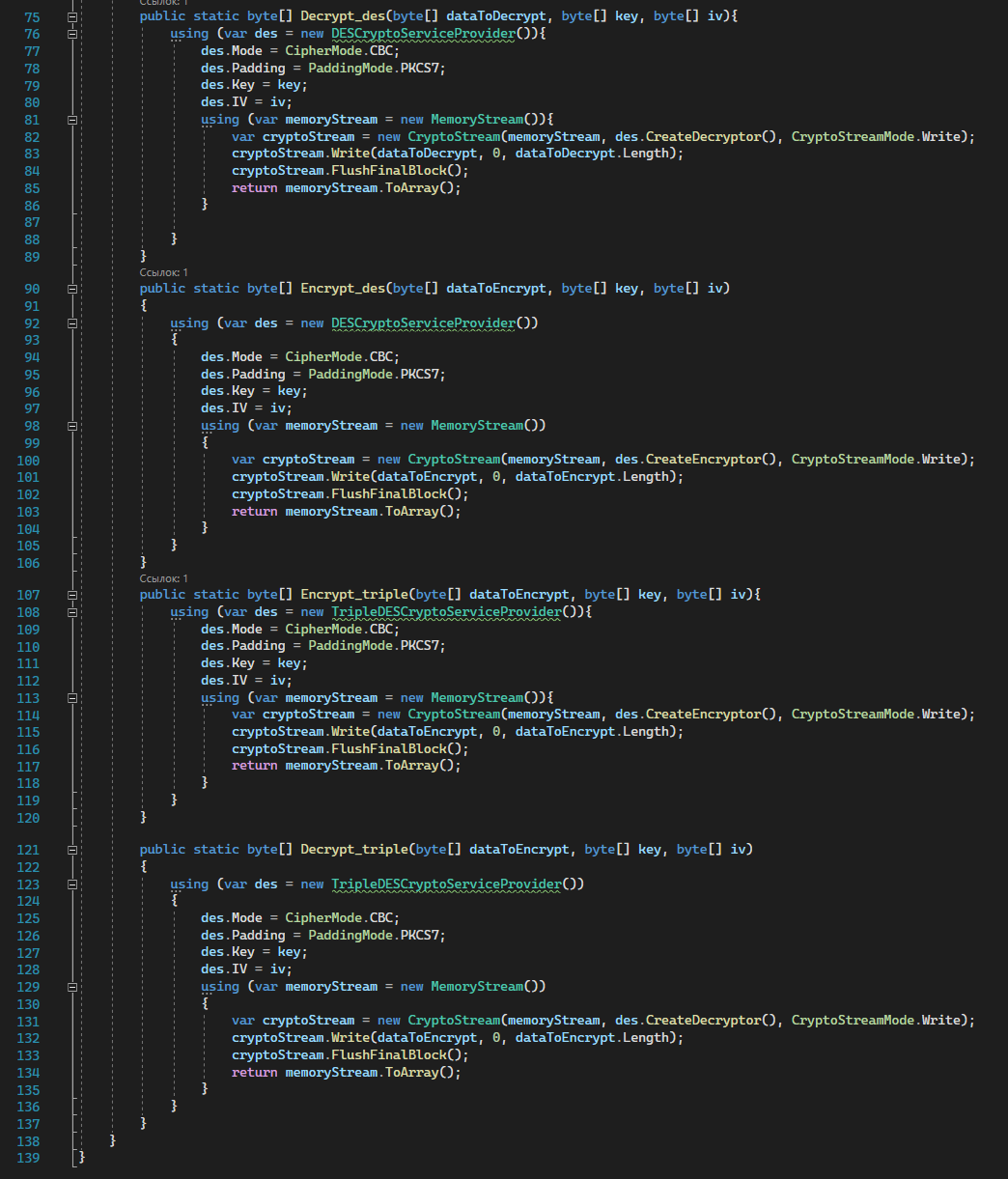
2) Небезпека, якщо злочинець дізнається секретний ключ

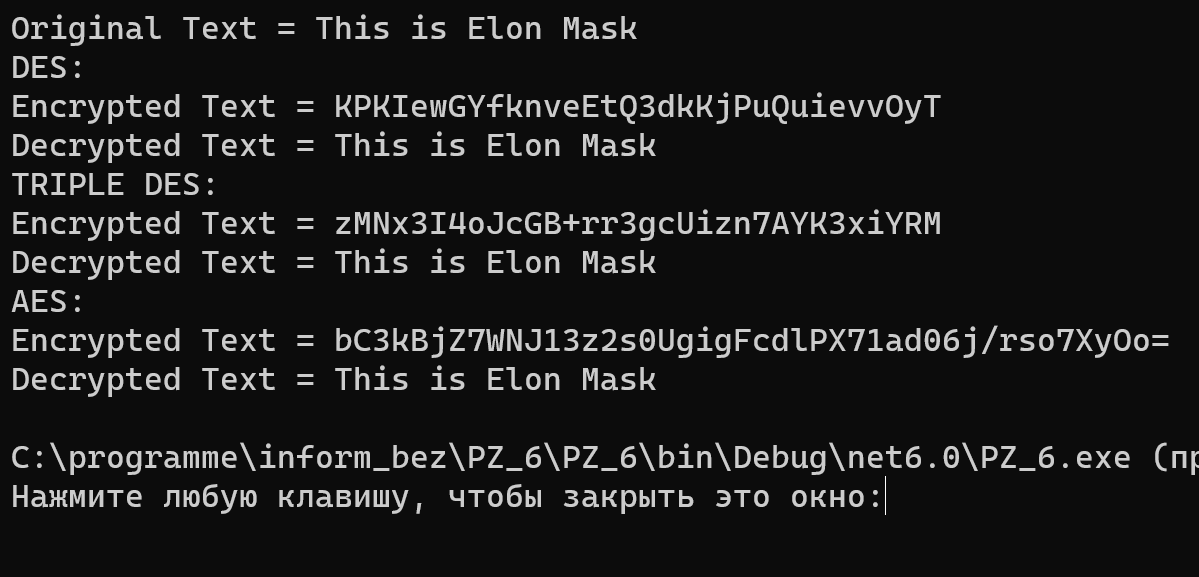
Шифрування у DES відбувається 64-бітними блоками (Рис. 2), де вхідні розділяються на 8-ми байтові (64-бітні) ланки, які зашифровуються з використанням 56-бітного секретного симетричного ключа для забезпечення конфіденційності. AES : розмір блоку 128 біт, довжина ключа 128, 192 або 256 біт й кількістm раундів 10, 12 або 14 в залежності від довжини ключа.

Раніше DES був надійний алгоритм, проте з годами комп’ютери стали більш потужними, тому brute-force атаки стали більш швидкими, тому на даний момент рекомендують використовувати AES.

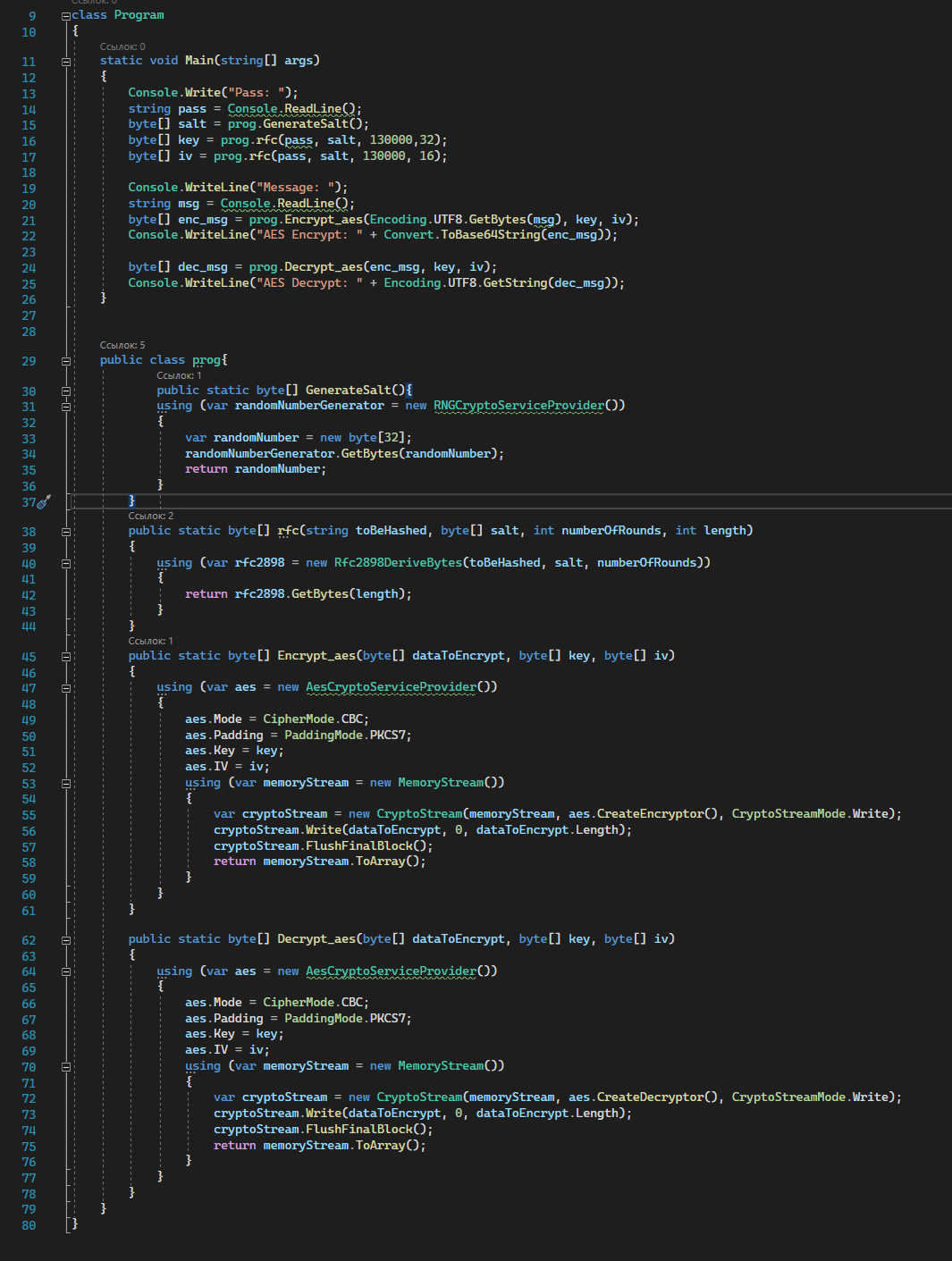
1) Написати програму, яка виконує зашифровування та розшифровування даних з використанням алгоритмів симетричного шифрування DES, Triple-DES, AES. Секретний ключ та вектор ініціалізації генерується випадковим чином.

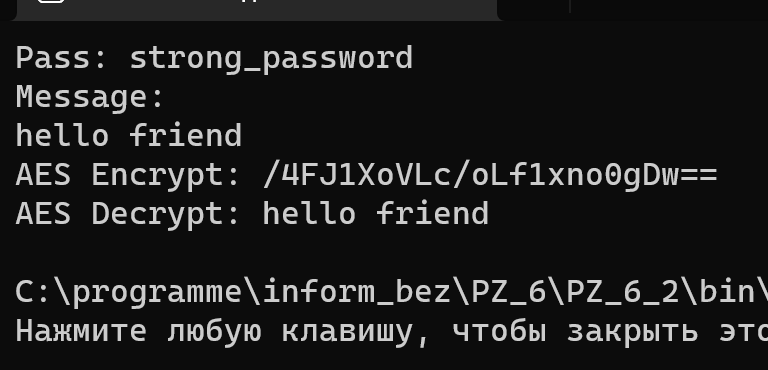






2) Для програми з п.1. реалізувати можливість задання секретного ключа та вектора ініціалізації за допомогою псевдовипадкової послідовності із використанням пароля. «Сіль» генерувати як випадкову послідовність байтів. Число ітерацій = номер варіанта \* 10'000. **Підказка**: використовувати клас *Rfc2898DeriveBytes*)





Висновок: Отже, ми дослідили шифрування DES, Triple DES, AES та зробили висновки щодо надійності таких алгоритмів.