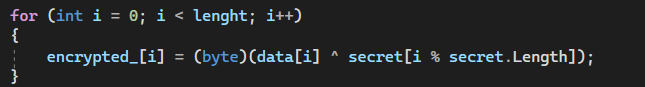
**“Реалізація шифру Вернама”**

Практичне заняття №2

Виконав: Черевач Юрій Аналолійович

1. Шифрування

Шифр Вернама



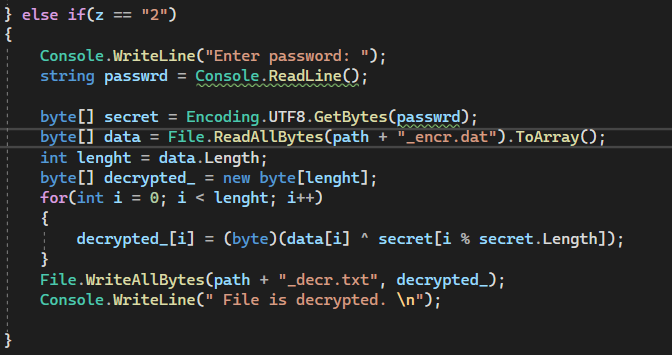
Цей цикл безпосередньо виконує шифрування.

Як відбувається шифрування:



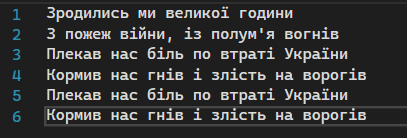
Ми читаємо пароль, беремо байти, також читаємо вмість нашого файлу, і по циклу проходимо по значеннях у файлі (тому важливо орієнтуватися на довжину файлу). Зашифровані данні записуються у новий файл із розширенням .dat.

Дешифрування відбувається схожим чином. Але зараз нам важливо мати правильний пароль, інакше дешифрування може відбутися некоректно. Наш код:

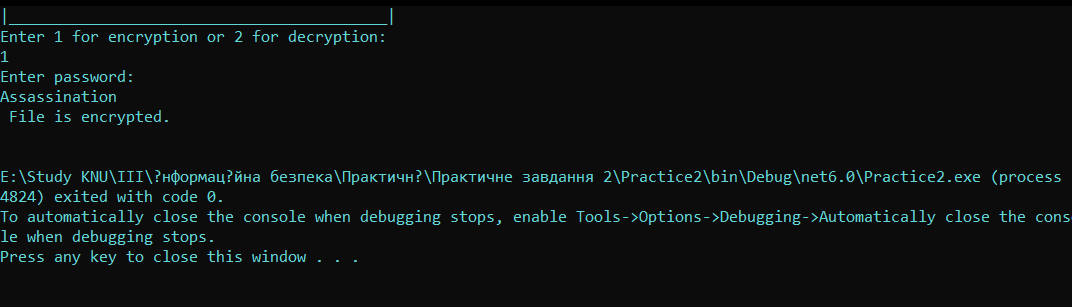


Процес такий само, але тепер дешифровані данні записуються у текстовий файл.

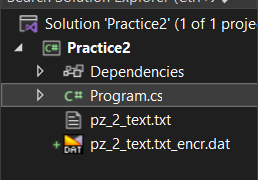
Тепер перевіримо, як працює все це на практиці. Ось наш текст:



Зашифруємо його у файл .dat і використаємо пароль “Assassination”.

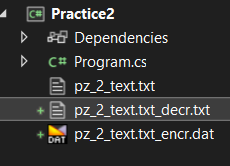


Бачимо, що у нас з’явився новий файл .dat.

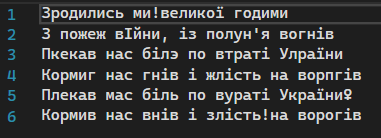


Спробуємо дешифрувати цей файл, але пароль введемо трішки інший, і побачимо, як дешифрується цей текст.

Введемо пароль “Assassinatioo” (довжину зберігаємо). Зауважте, що ми змінили лише один знак. Бачимо, що у нас з’явився дешифрований текстовий файл.

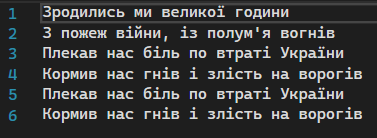


Але текст дещо не той, який був початково.



Тобто, риси початкового тексту впізнати можливо, але змінивши лише один символ в паролі ми отримали некоректний результат. Зараз розшифруємо з нормальним паролем “Assassination”.

Як бачимо, текст коректно дешифрувався. Отже, все спрацювало.



Висновок: виконуючи практичне завдання №2 я ознайомився з реалізацією шифра

Вернама та навчився застосовувати ці знання для реалізації певних завдань за допомогою мови програмування С#.