**Звіт**

**до предмету «Основи інформаційної безпеки»**

Студента Київського Національного Університету ім. Тараса Шевченко

Пруніча Сергія Миколайовича

Факультет інформаційних технологій

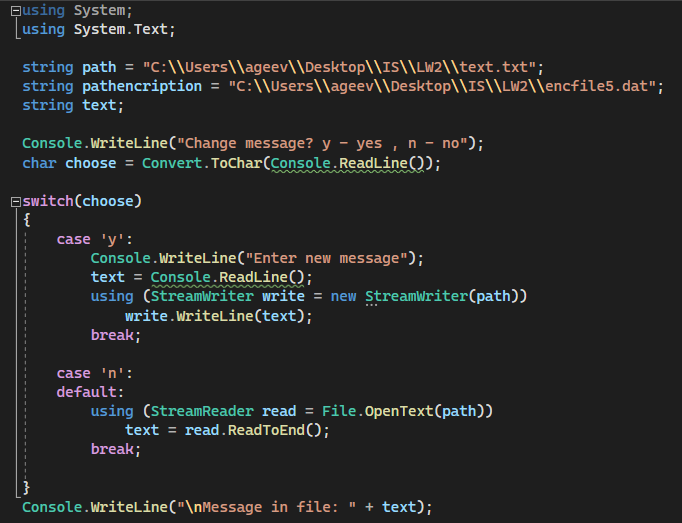
Група МІТ-21



Лабораторна робота №2

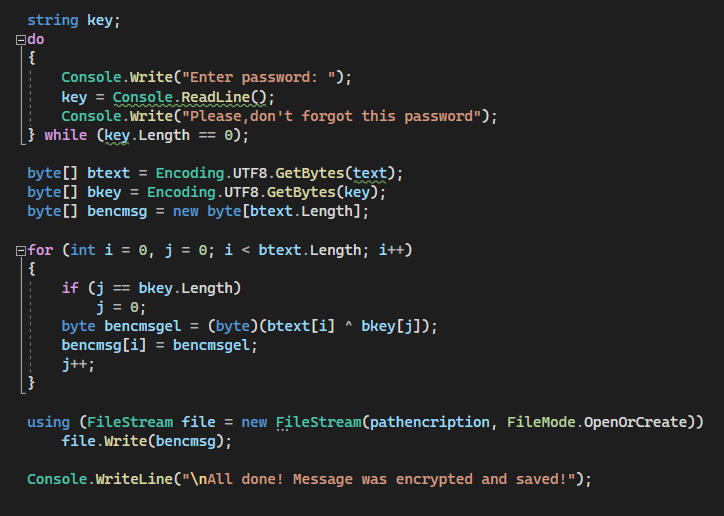
Тема: «Реалізація шифру Вернама»

1. Створити програму для зчитування файлу, шифрування його вмісту та запису зашифрованого файлу у ту ж саму папку але з розширенням \*.dat.



Спочатку ініціалізую змінні path(шлях звідки береться повідомлення), pathencription(шлях куди буде збережено зашифроване повідомлення з розширенням .dat) та text(саме повідомлення яке буде шифруватися)

Запитую у користувача чи бажає він змінити інформацію у файлі(якщо відповідь так, тоді запрошується нове повідомлення та зберігається у файлі, інакше береться наявне повідомлення з файлу)

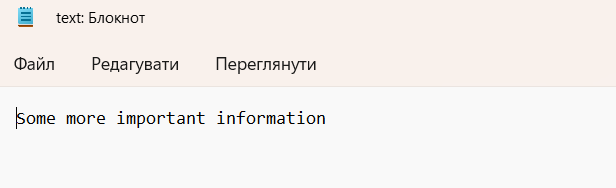


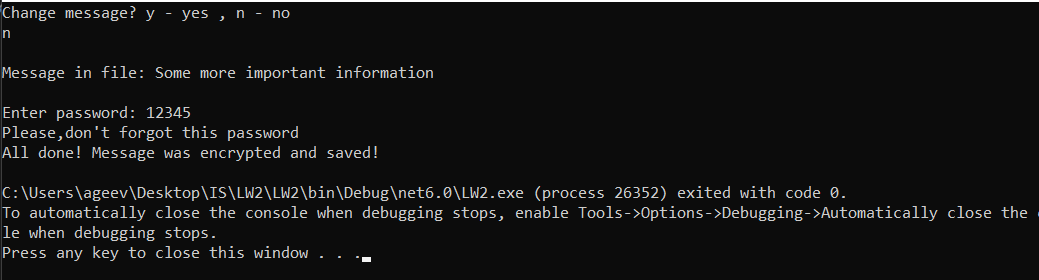
Запрошуємо у користувача ключ, за допомогою якого буде виконано шифрування.

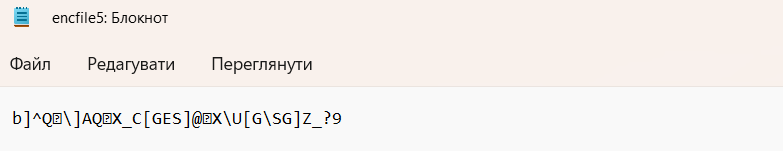
Зберігаємо ключ та текст повідомлення у вигляді масиву

За допомогою циклу for шифруємо кожен біт масиву повідомлення

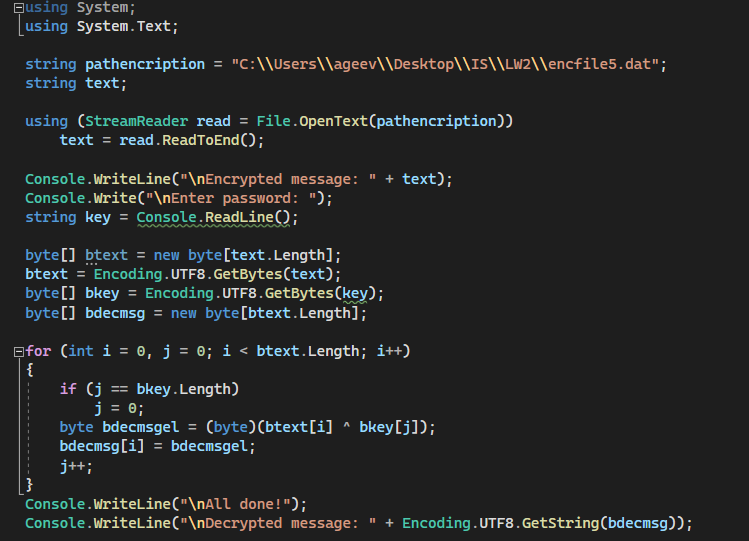
Після виконання циклу записуємо результат у потрібний файл







1. Модифікувати програму так, щоб можна було розшифровувати зашифрований файл.



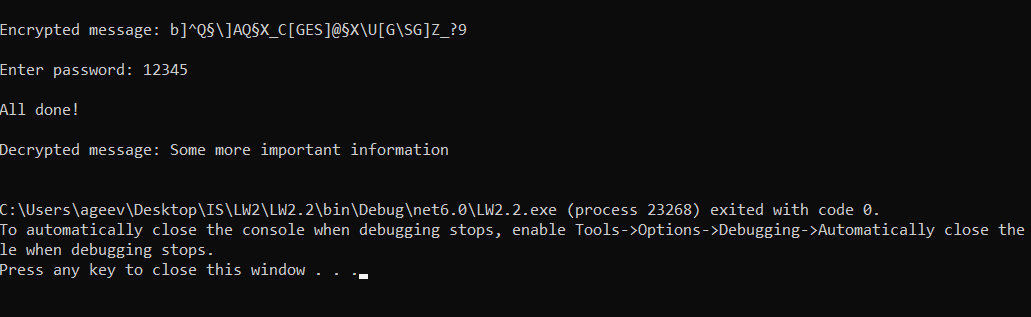
Спочатку ініціалізую змінні pathencription(шлях до файлу з зашифрованим повідомленням) та text(змінна яка бути тримати в собі повідомлення)

У зміну text зчитуємо зашифроване повідомлення з файлу

Також запрошуємо у користувача такий самий пароль як і для шифрування.

Записуємо змінні у масив та за допомогою цикла for проводимо дешифрування

По закінченню виводимо на екран повідомлення про успішно розшифроване повідомлення, а також саме повідомлення на екран



**Висновок:** в ході практичної роботи ми навчились використовувати операцію XOR та навчились застосовувати її для шифрування вмісту файлів і відповідно розшифрування зашифрованого вмісту файлу.