***Практичне заняття №2***

*«Реалізація шифру Вернама»*

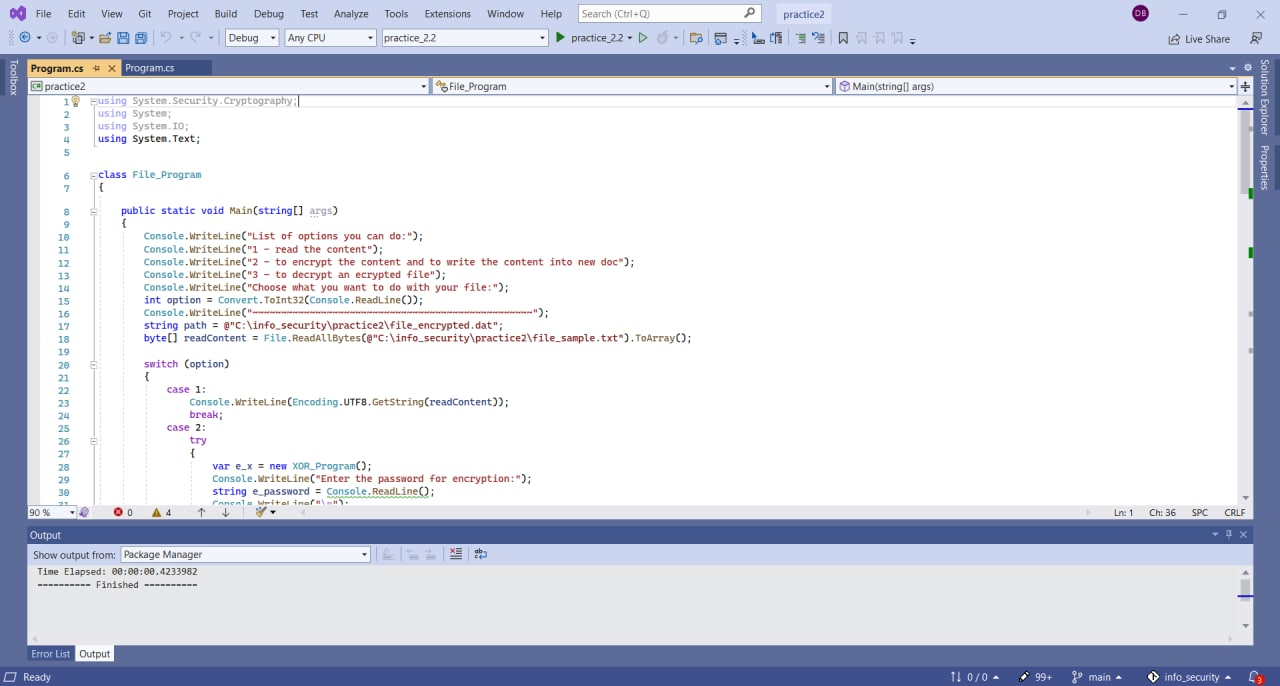
Виконала студентка групи МІТ-21 **Борук Дарина**

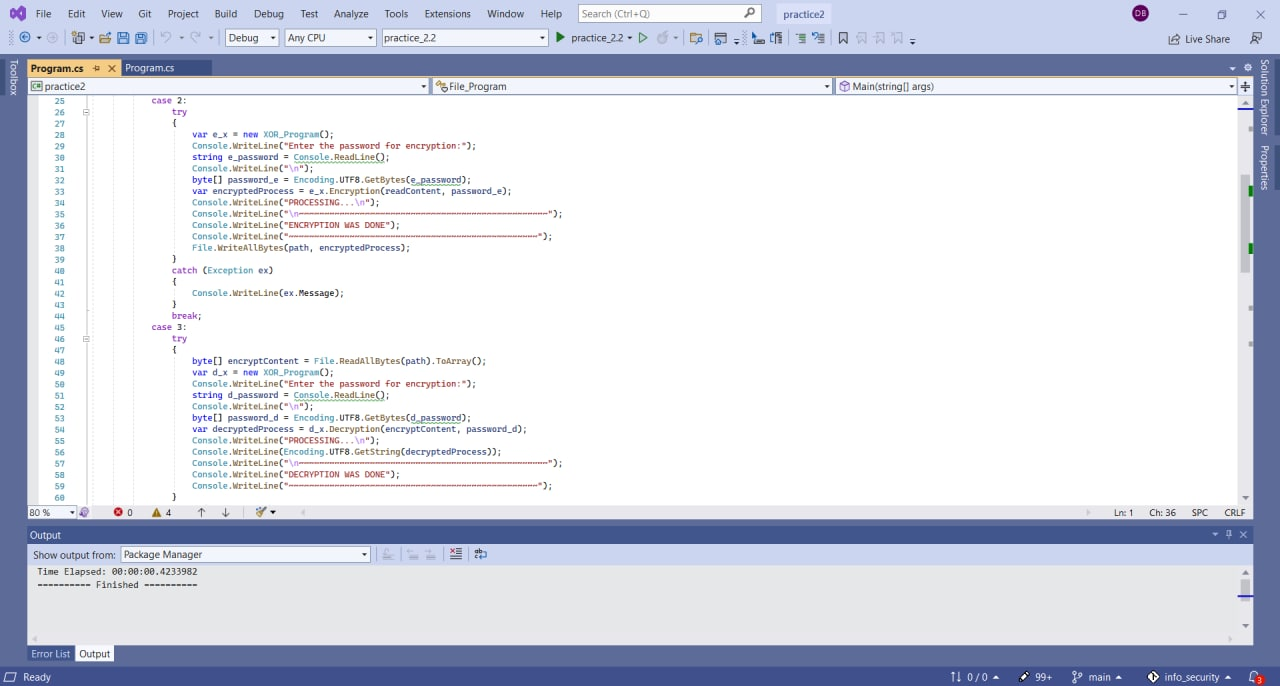
Мета: розібратися із шифром Вернама, розглянути операцію «виключне АБО» та написати програми для шифрування файлу даним шифром, його розшифрування та дешифрування.

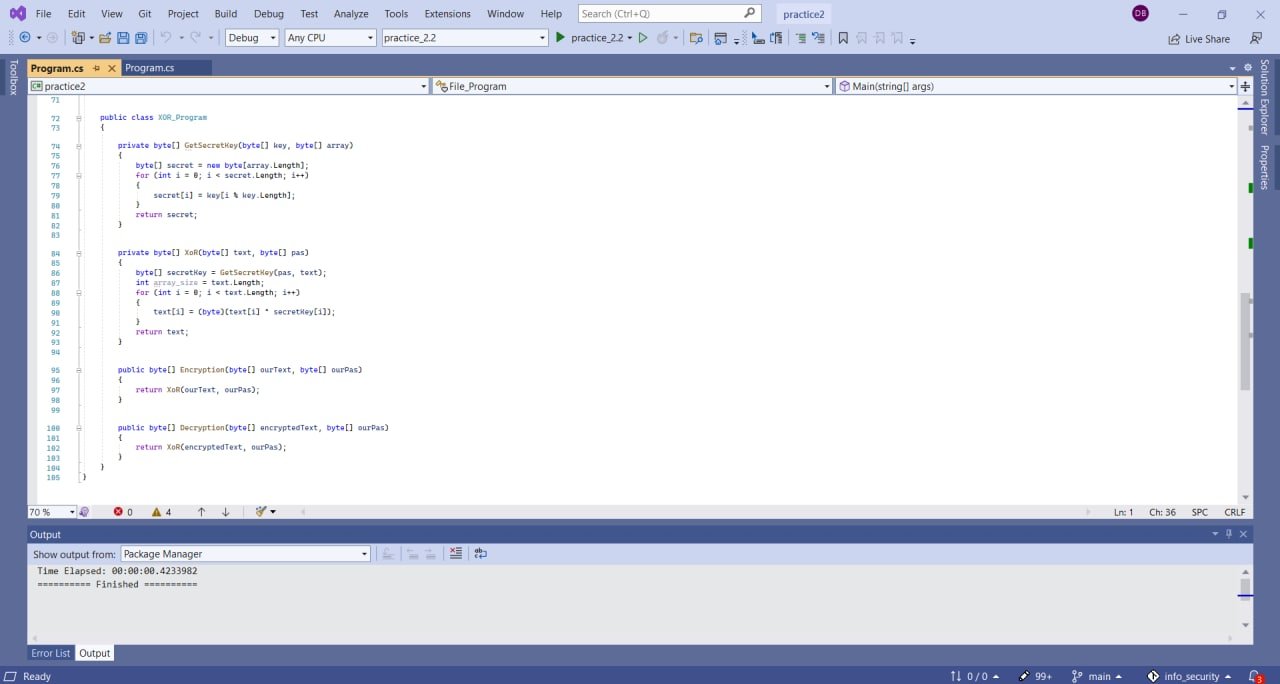
Хід роботи:

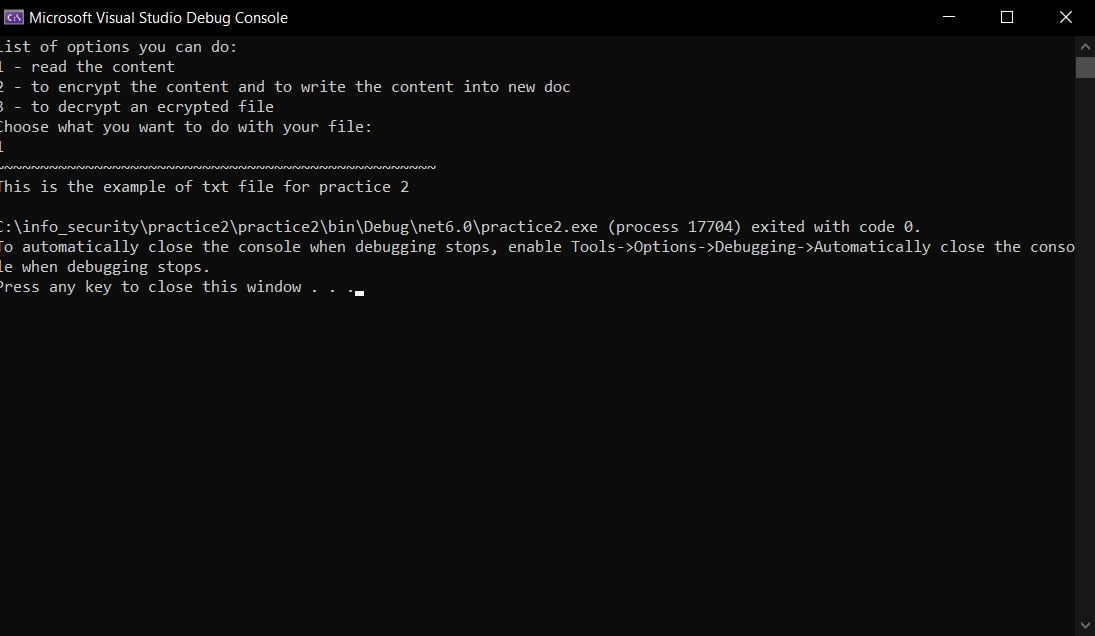
* Розглянемо спочатку перше і друге завдання: створити програму для зчитування файлу, шифрування його вмісту та запис зашифрованого файлу у ту ж саму папку з розширенням .dat; модифікувати програму, щоб можна було розшифрувати зашифрований файл

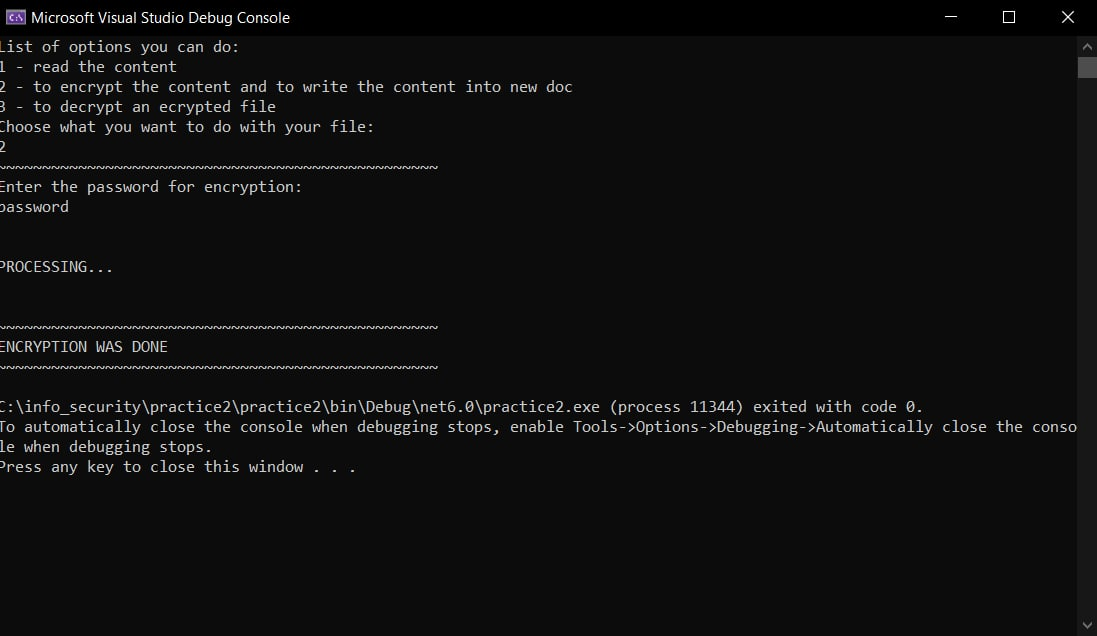
1. Першим діло після створення нашого солюшна підключимо простір імен System.Security.Cryptography, System.IO, System.Text і System. Далі створимо нашу головну функцію Main і забезпечити вибір користувача за допомогою менюшки.
2. У кінці створюємо методи для отримання нашого шифру Вернама. Створюємо окремий клас і в ньому пишемо наші методи: щоб отримати секретний ключ, його застосування для безпосередньої операції «виключне АБО» і для подальшого шифрування і дешифрування.
3. Далі я створила файл у папці з нашим проектом, у який будемо записувати вміст нашого зашифрованого файлу, і додала його шлях у змінну path.
4. Далі робимо switch для вибору користувача: 1 – для простого зчитування мого текстового документа для шифрування, 2 – для його шифрування і запису вмісту у новий файл, розшифрувати цей новий файл.
5. Розглянемо 2 вибір. Створюємо об'єкт нашого класу для операції шифрування. Користувач вводить пароль, який ми «перетворюємо» у масив байтів. Потім зчитуємо вміст мого файлу для 1ого завдання і так само переводимо його у масив байтів. Далі ми передаємо масив байтів вмісту файлу і масив байту нашого паролю у функцію для шифрування. Спочатку пароль передаємо функції для генерації ключа і генеруємо його такої ж довжини, як і довжина вмісту файлу, і потім безпосередньо застосовуємо функцію XOR до нашого вмісту і до нашого ключа. У кінці повертаємо результат цієї операції у вигляді нового файлу із зашифрованим текстом.
6. У разі розшифрування ми виконуємо ті ж самі дії, що і в пункті 5, але замість мого файлу ми беремо наш новий зашифрований файл, а пароль використовуємо той самий. У результаті виконання виводжу на екран наш розшифрований вміст файлу.

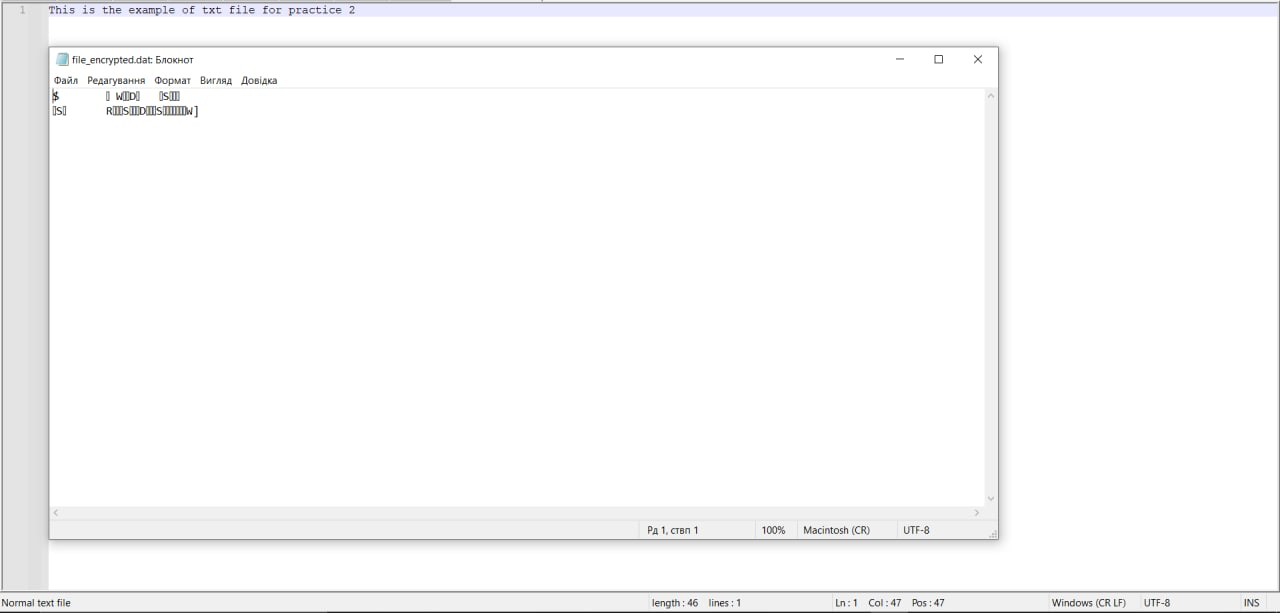


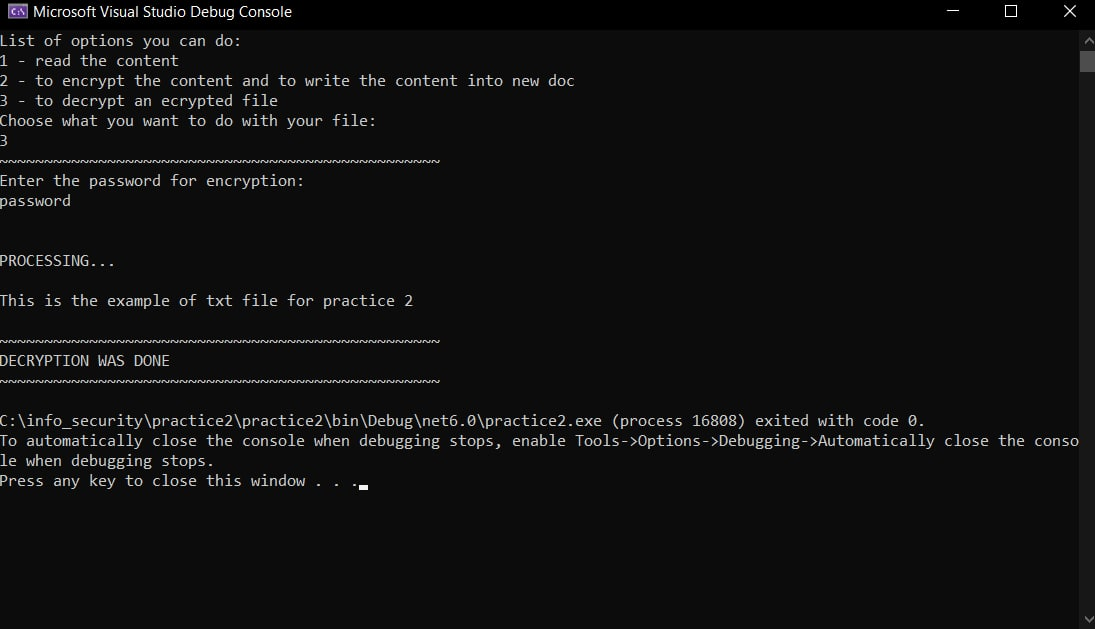






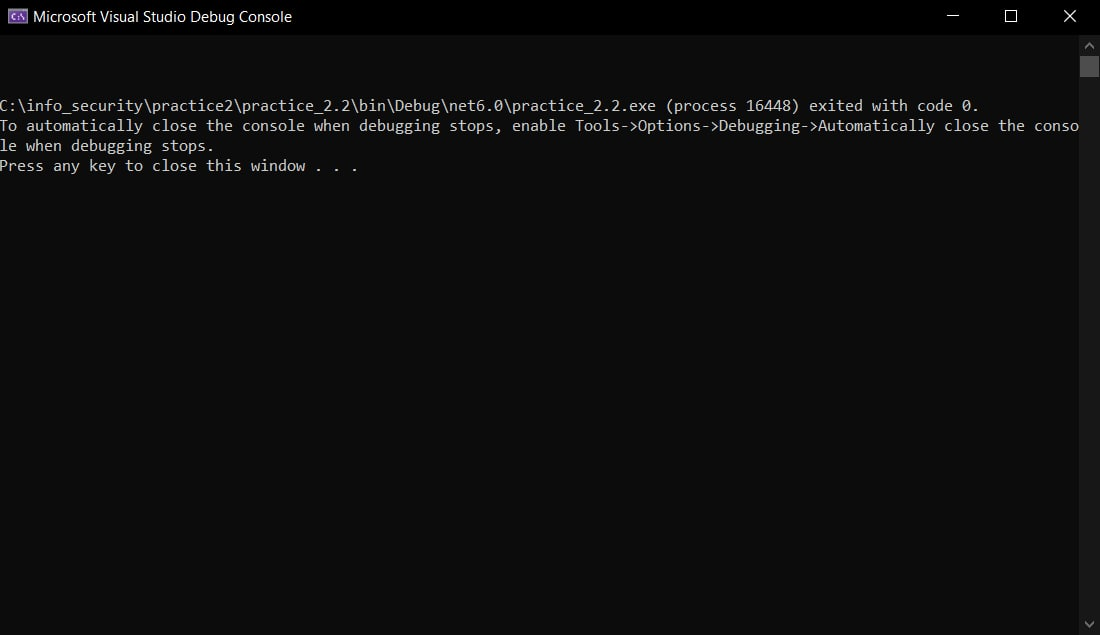


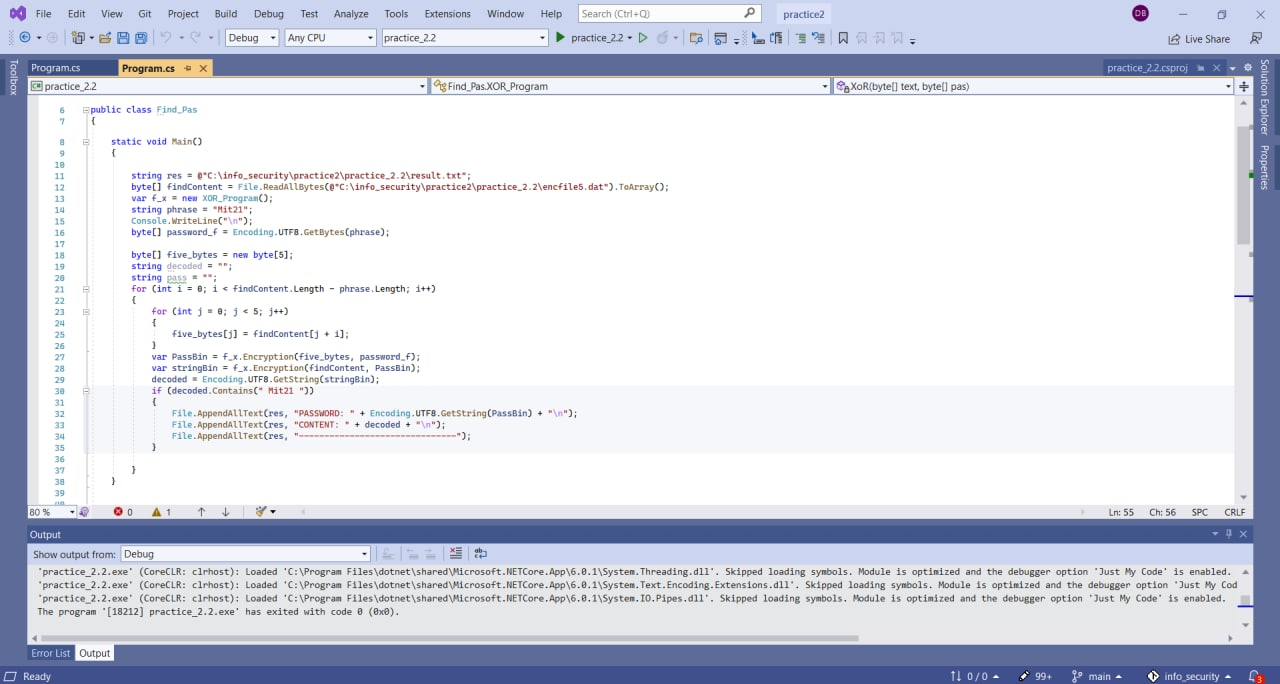


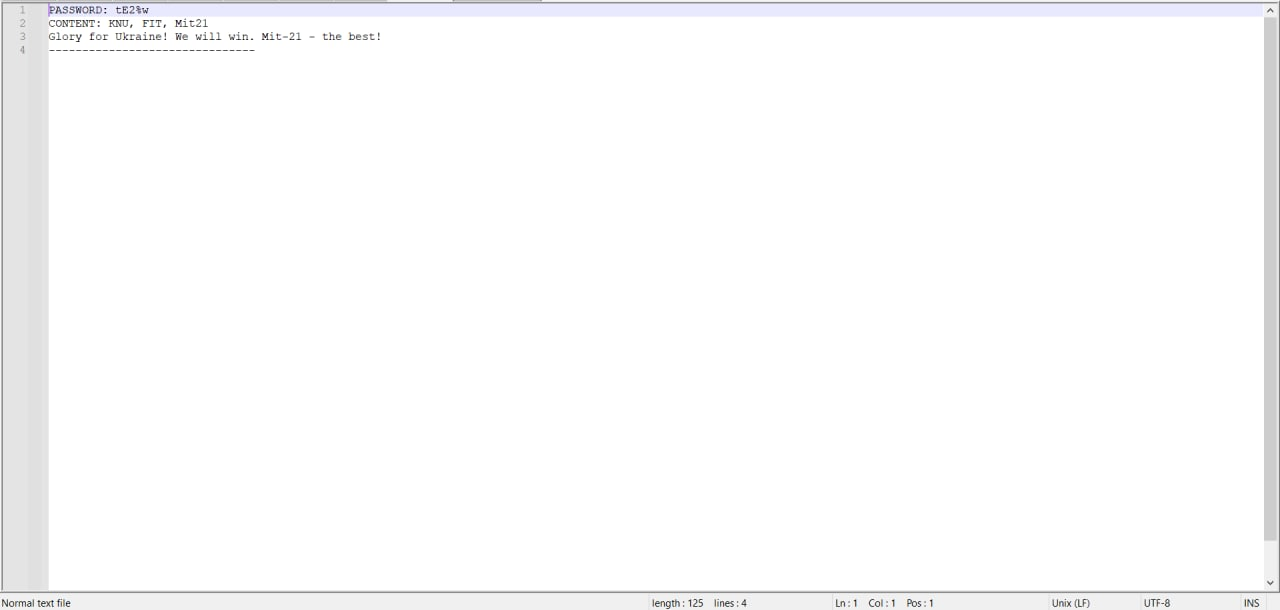


* Тепер розглянемо 3 завдання для дешифрування зашифрованого файлу методом перебору (знаємо, що пароль складається із 5 символів, а вміст файлу містить в собі фразу «Mit21»)

1. Підключаємо ті ж самі простори імен, що і в попередній задачі і створюємо головну функцію Main. Так само включаємо усі функції для генерації шифру Вернама, що були використані у попередній задачі також.
2. Спочатку ми зчитуємо уміст нашого зашифрованого файлу і переводимо його у масив байтів. Потім ми додаємо змінну phrase і даємо їй значення нашої фрази «Mit21».
3. Далі створюємо об'єкт класу для генерації XOR і створюємо змінну у масив байтів і даємо їй значення нашої фрази. Ми знаємо, що операція XOR має таку властивість: якщо розшифровану частину файлу накласти на зашифровану частину, місця їх сходження видасть нам шматочок паролю. Тому наша фраза є таким шматочком і ми будемо підставляти її у наш файл, зміщуючи на один символ по черзі. Потім ми будемо перевіряти наш дешифрований текст на наявність нашої фрази, і якщо він буде місити її в собі, то ми записуємо цей текст і пароль до нього у створений файл, якщо ні – то пропускаємо і йдемо далі підбирати. Таким чином, ми зможемо дійти точки сходження нашої фрази і отримаємо і пароль і наш дешифрований файл.







Висновки: у ході практичного заняття були отримані навички писання мовою C#, а саме: вміння написати програми для шифрування методом «виключне АБО» (шифром Вернама), вміння написати програми для розшифрування файлу і дешифрування невідомого нам файлу методом підбору паролей.