***Практичне заняття №2***

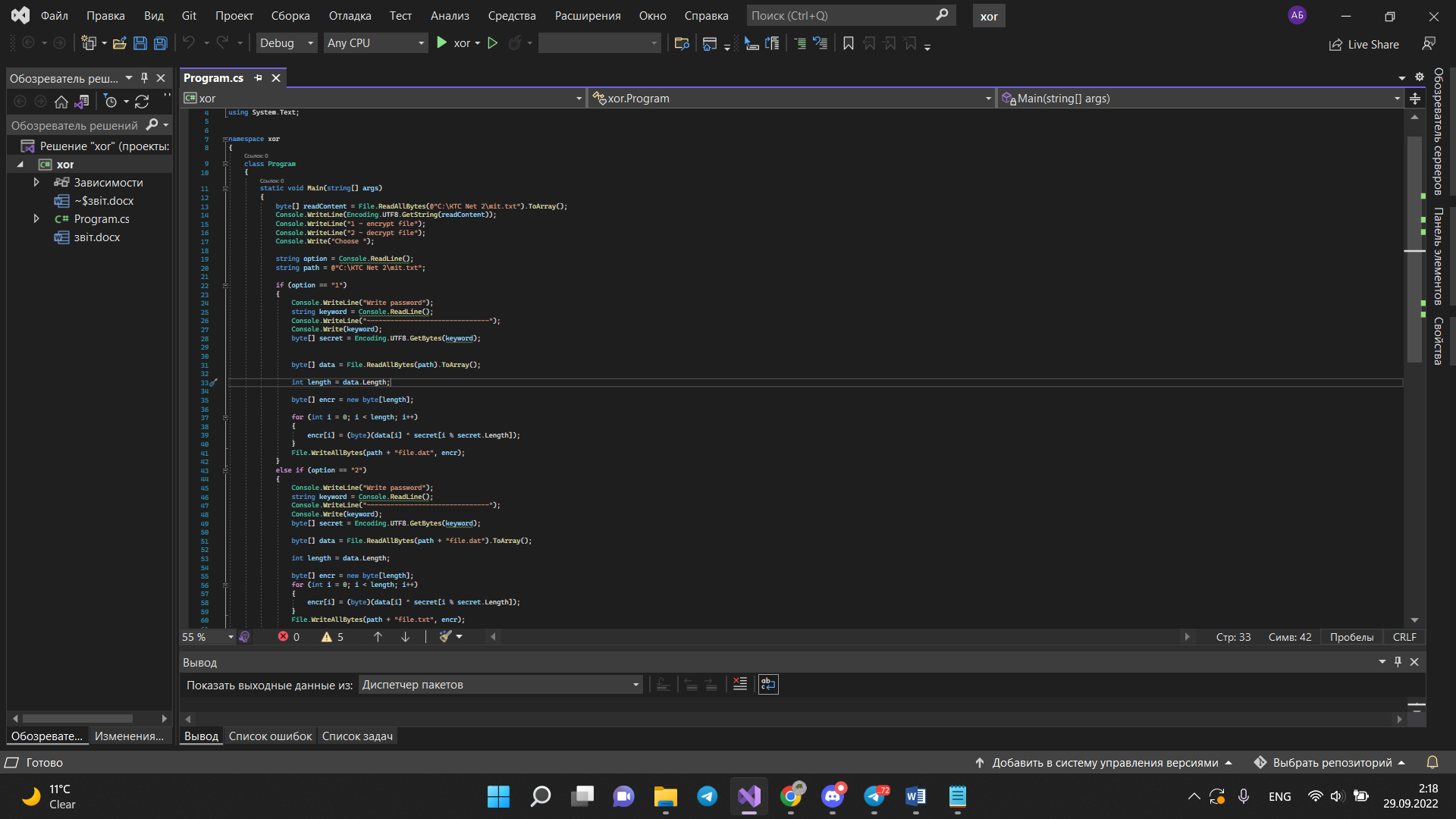
*«Реалізація шифру Вернама»*

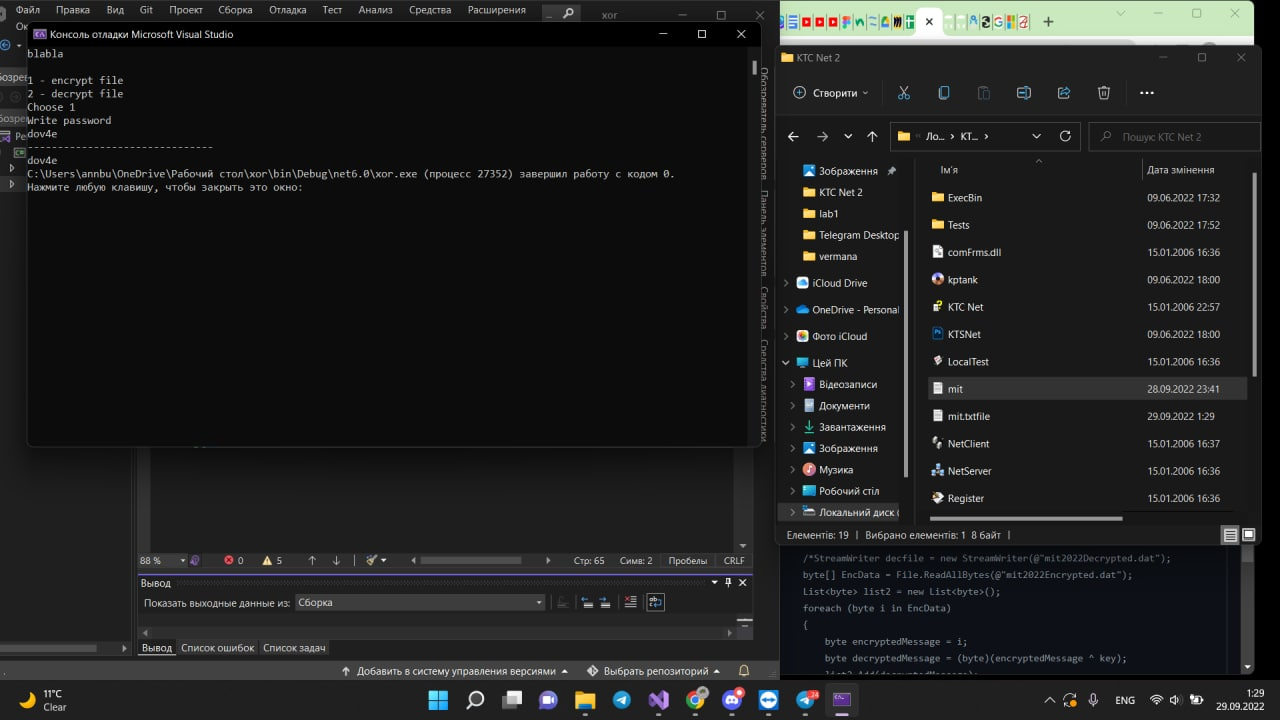
Виконала студентка групи МІТ-21 Булгакова Анна

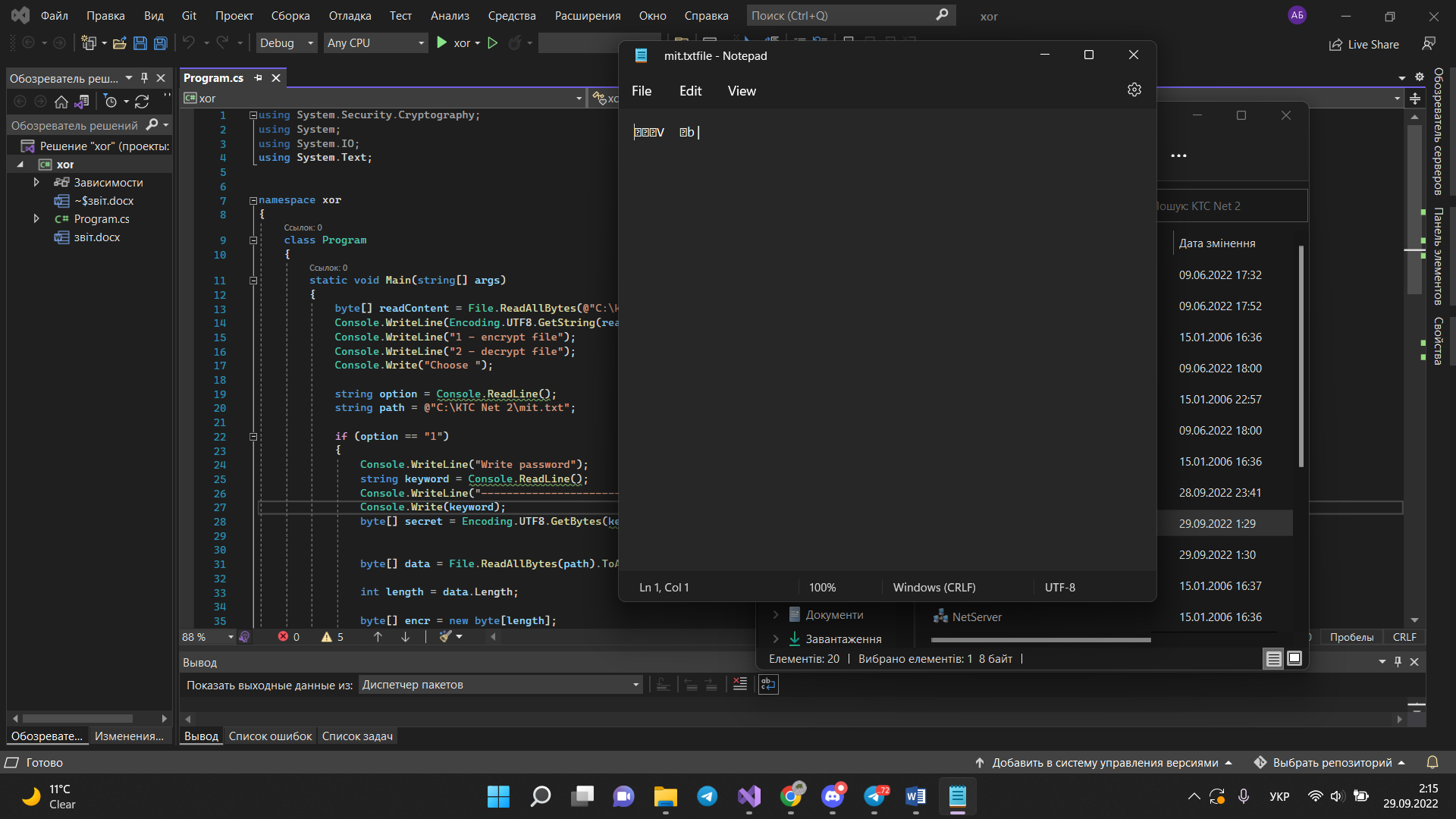
Завдання 1 Створити програму для зчитування файлу, шифрування його вмісту та запису зашифрованого фалу у ту ж саму папку але з розширенням \*.dat.

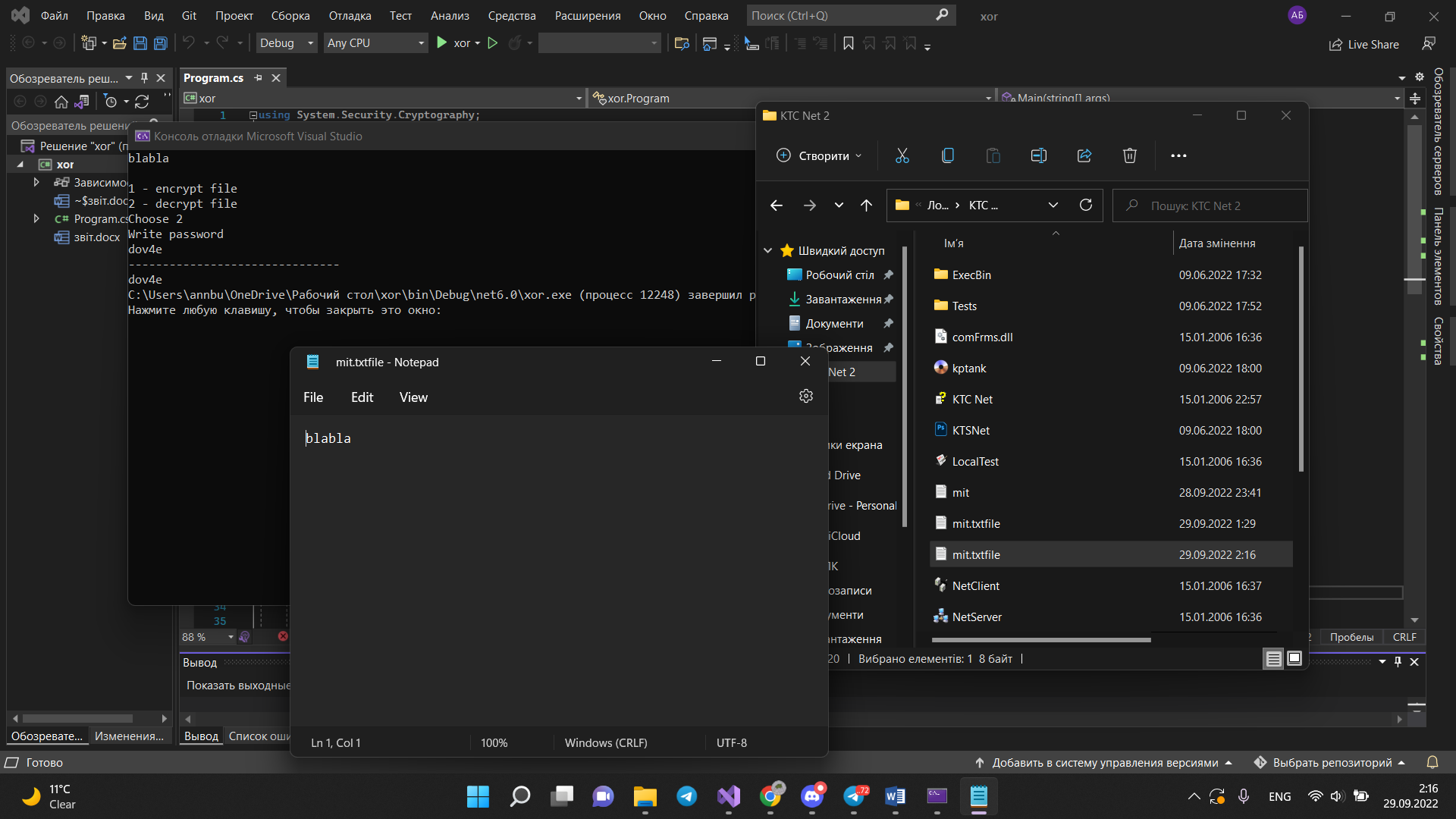
Завдання 2 Модифікувати програму так, щоб можна було розшифровувати зашифрований файл.

Завдання 3 Створити програму для дешифрування (не плутати з розшифруванням) зашифрованого файлу методом «грубої сили» або методом перебору із використанням апріорної інформації про зашифрований текст, а саме: довжина пароля – 8 символів; у тексті присутня фраза "Mit21".



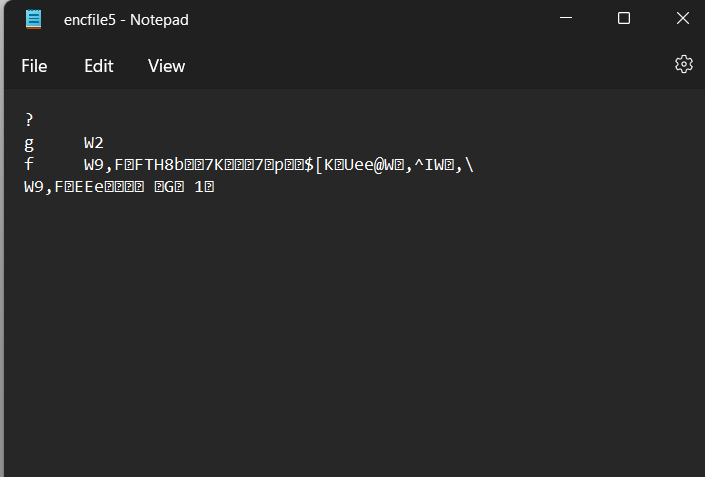


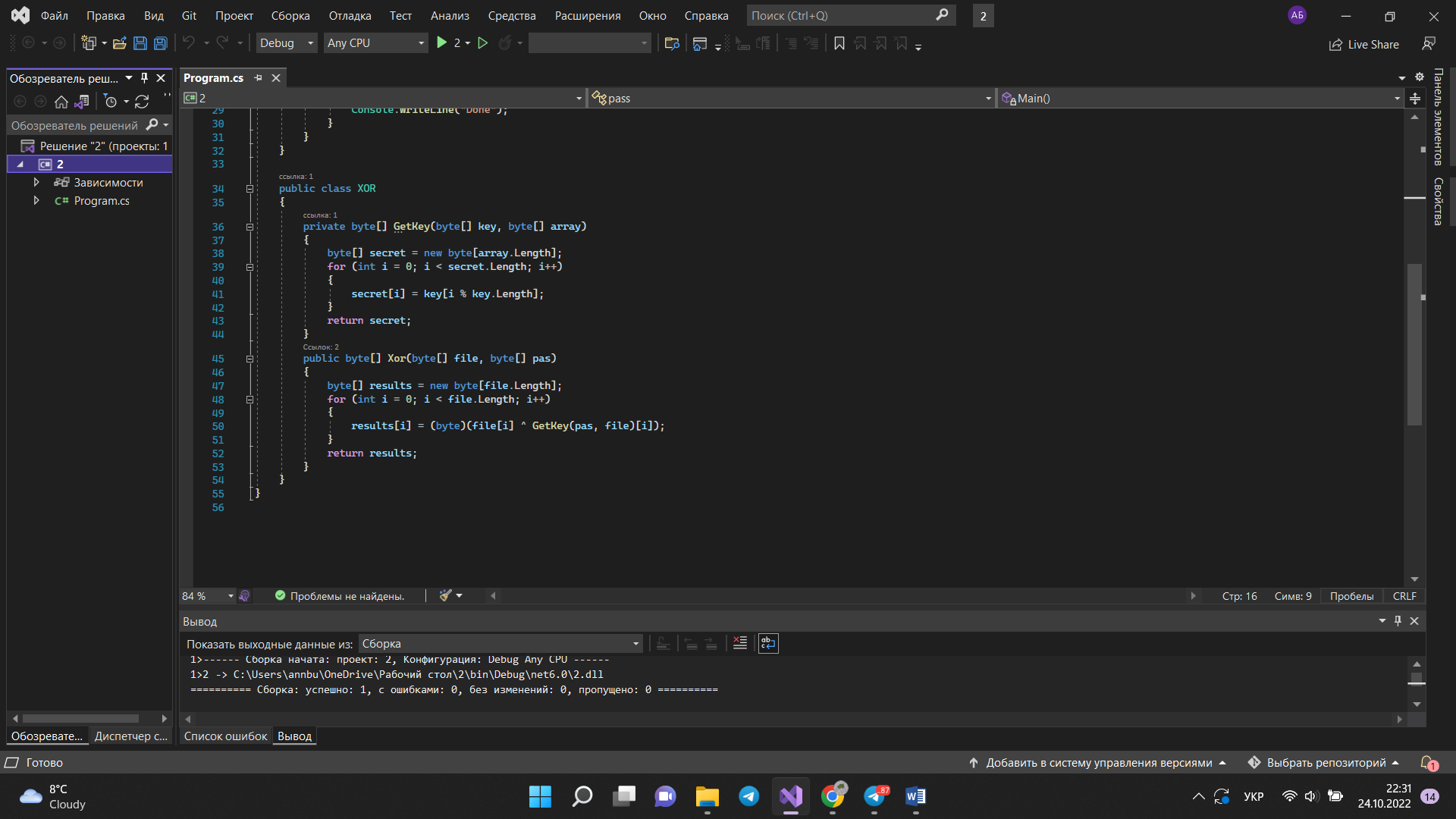
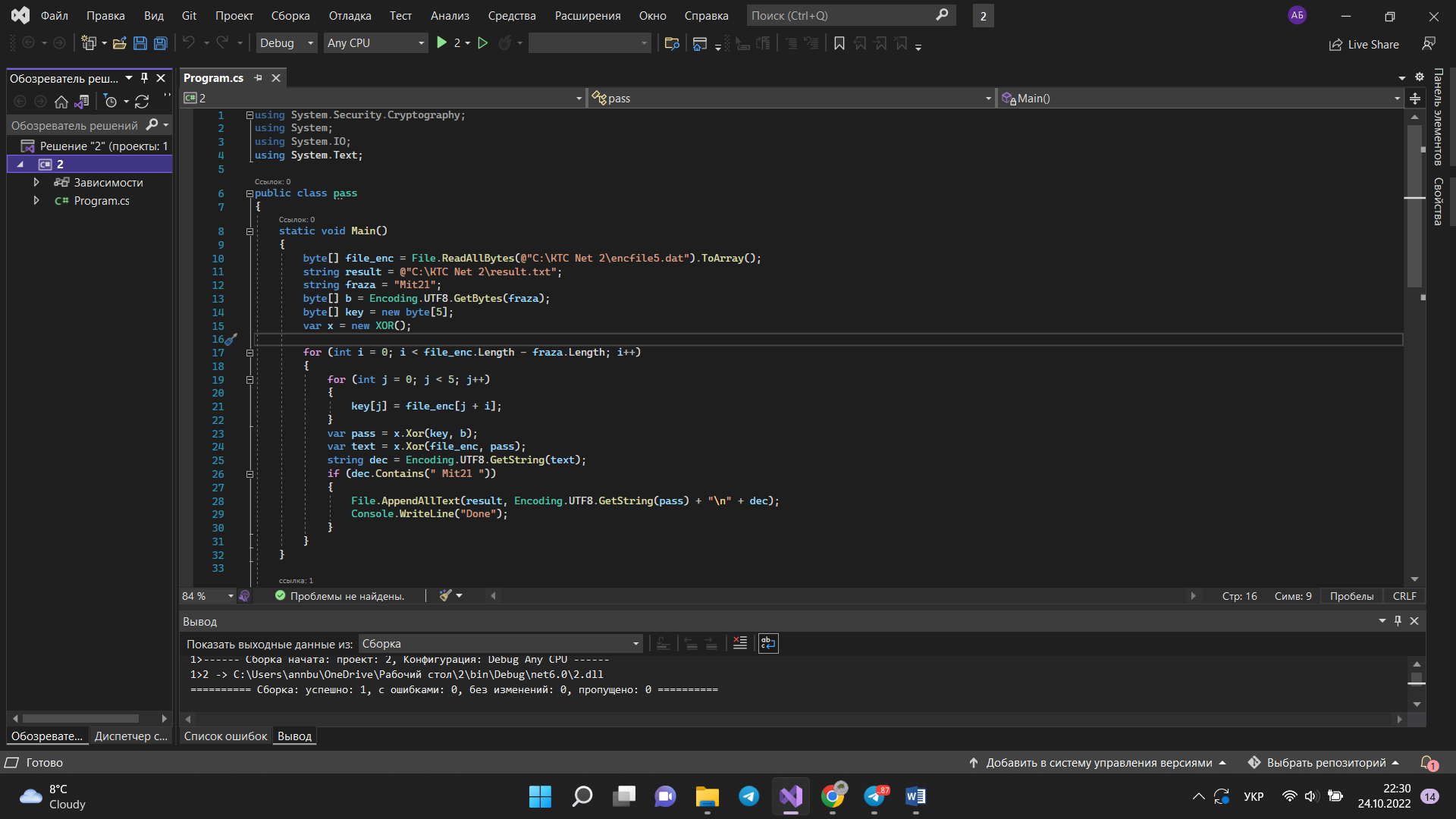
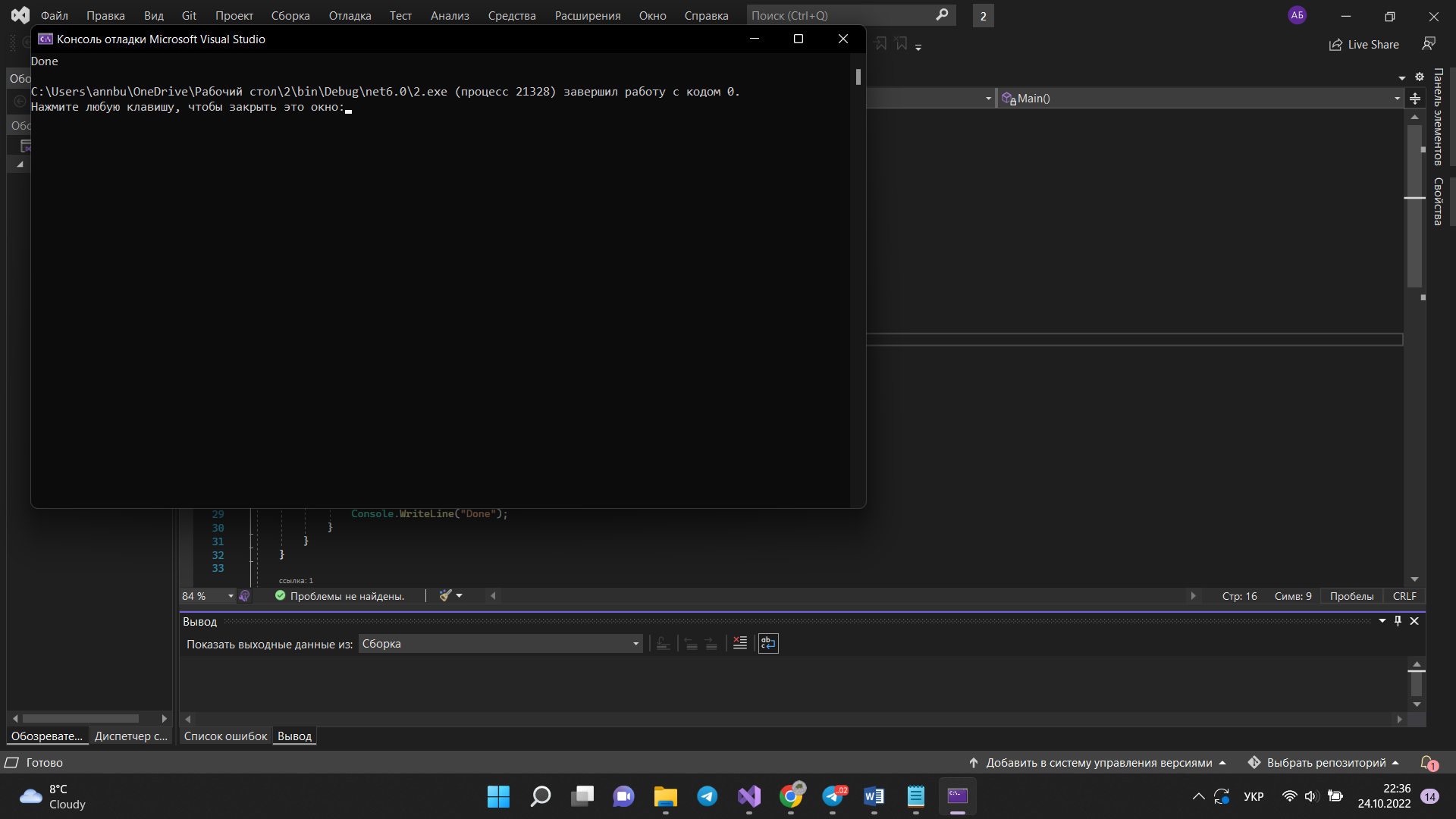
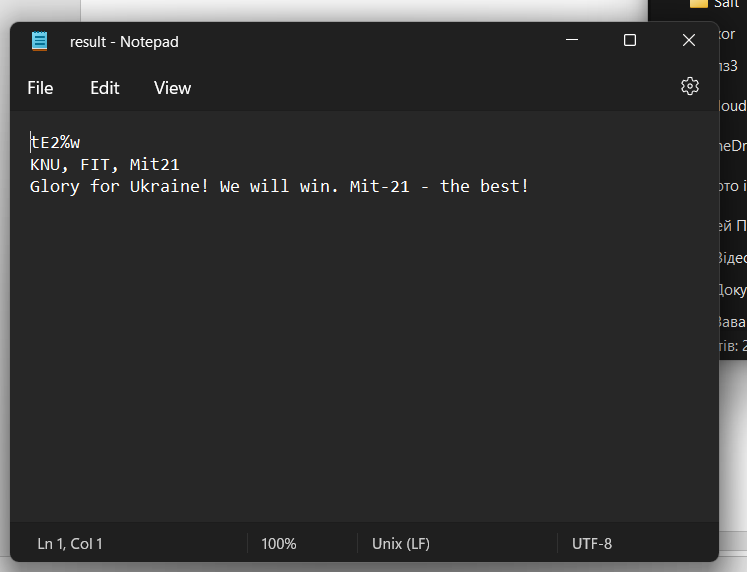




Виконавши перше завдання, після запуску коду в нас створюється документ (mittxtfile) з розширенням .dat та в нього записується зашифроване повідомлення з файлу mit.txt. Після виконання програмою другого завдання в папці створюється документ вже знову з розширенням .txt (також mittxtfile) та в нього вже записується розшифроване повідомлення.

**Завдання 3**





Створюємо функції для шифра Вермана(XOR).

XOR має таку властивість, що якщо шматочок не зашифрованого повідомлення накласти на ту саму частину зашифрованого, то можна отримати ключ. Тому за допомогою вкладеного (двовимірного) циклу перебираємо символи так щоб задана фраза наклалася, кожного разу перевіряючи дешифроване повідомлення на наявність цієї фрази. Якщо знаходимо, то записуємо пароль і повідомлення до файлу result.

У даній практичній роботі ми використовували шифр Вернама. Для шифрування рядка бітів необхідно мати ключ, що складається з тієї ж самої кількості двійкових знаків, що й повідомлення. Кожен біт рядка, що підлягає шифруванню, додається за модулем 2 (операція XOR) до відповідного біта ключа й отримуємо шифрограму.

Шифр Вернама є єдиною системою шифрування, для якої доведена абсолютна криптографічна стійкість.

**Висновок:** Отже, на даній практичній ми ознайомилися із шифром Вернама (XOR) та навчилися реалізовувати програму для шифрування і розшифрування методом «виключне АБО» (шифром Вернама, XOR), при цьому використовувавши текстові файли, та програму для розшифрування файлу і дешифрування невідомого нам файлу методом підбору паролей на С#.