***Практичне заняття №2***

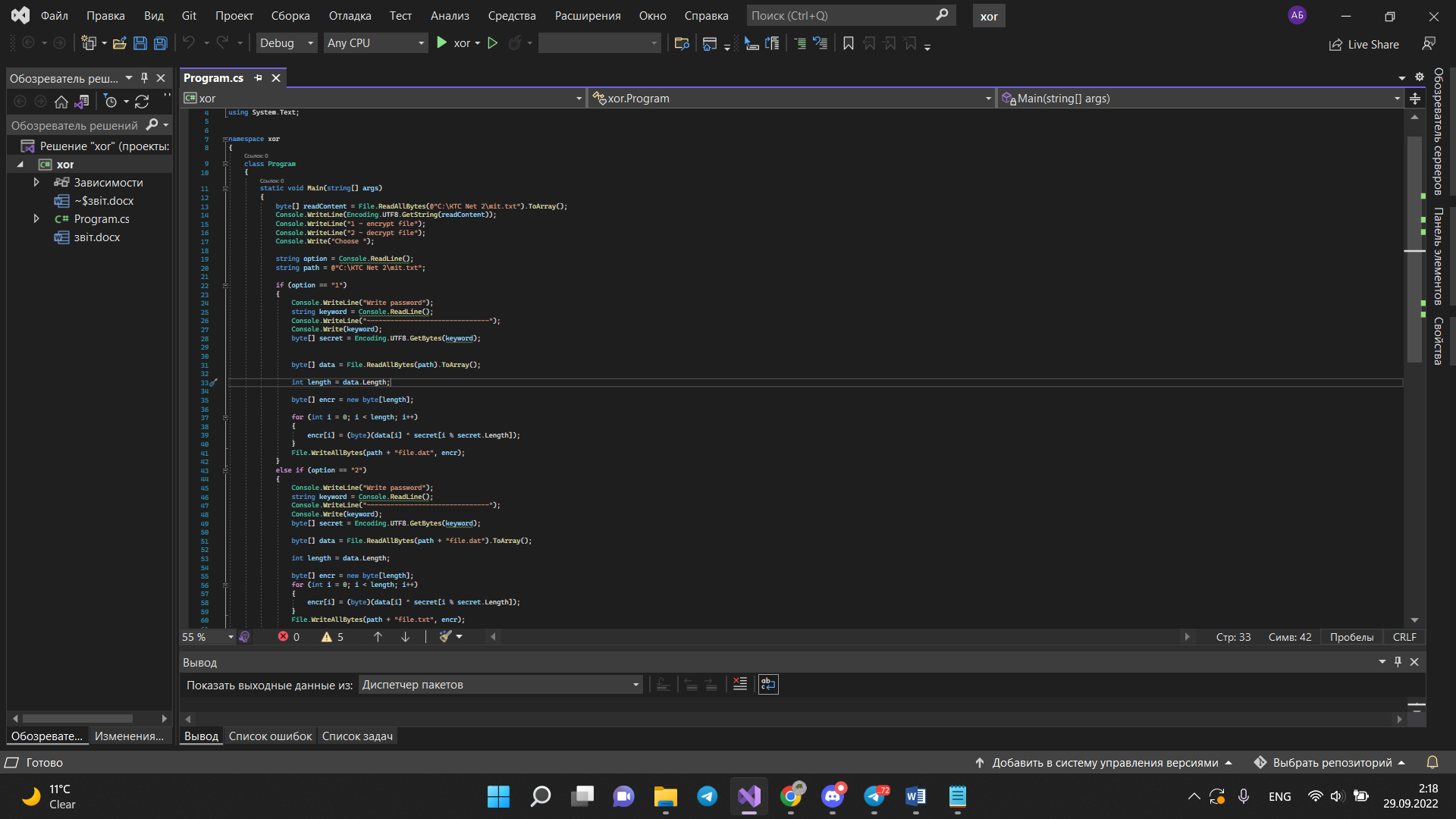
*«Реалізація шифру Вернама»*

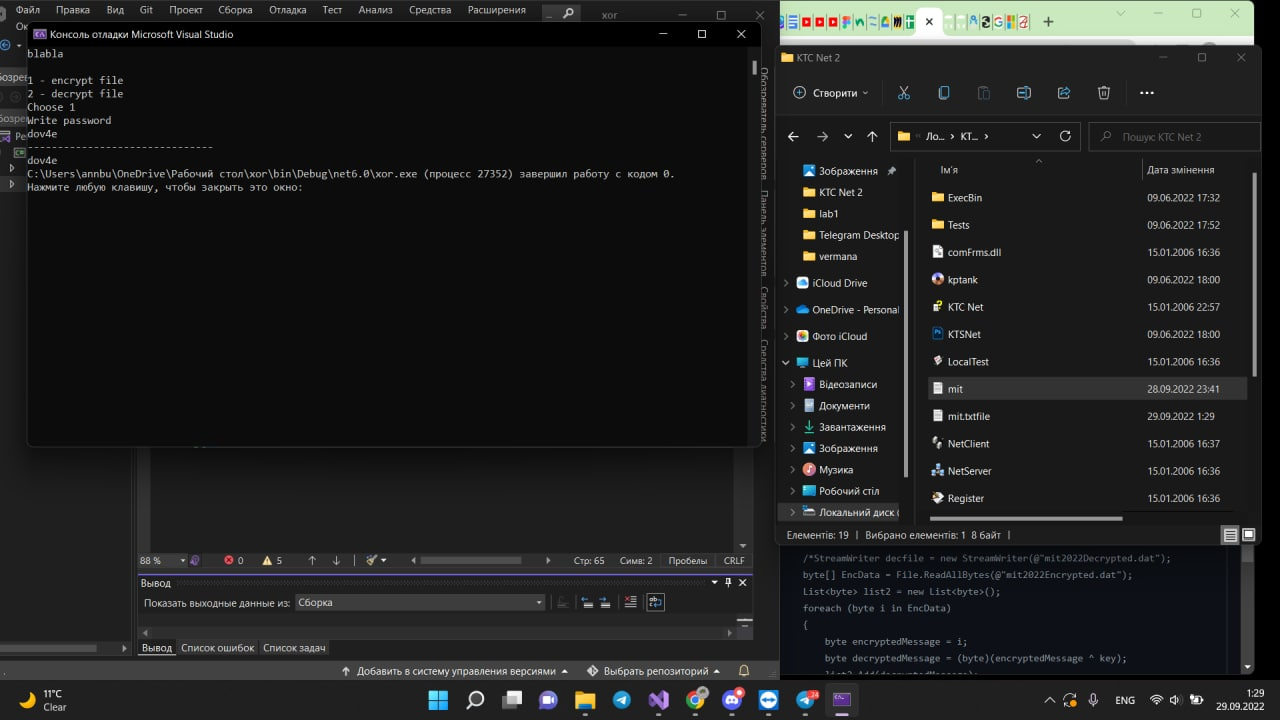
Виконала студентка групи МІТ-21 Булгакова Анна

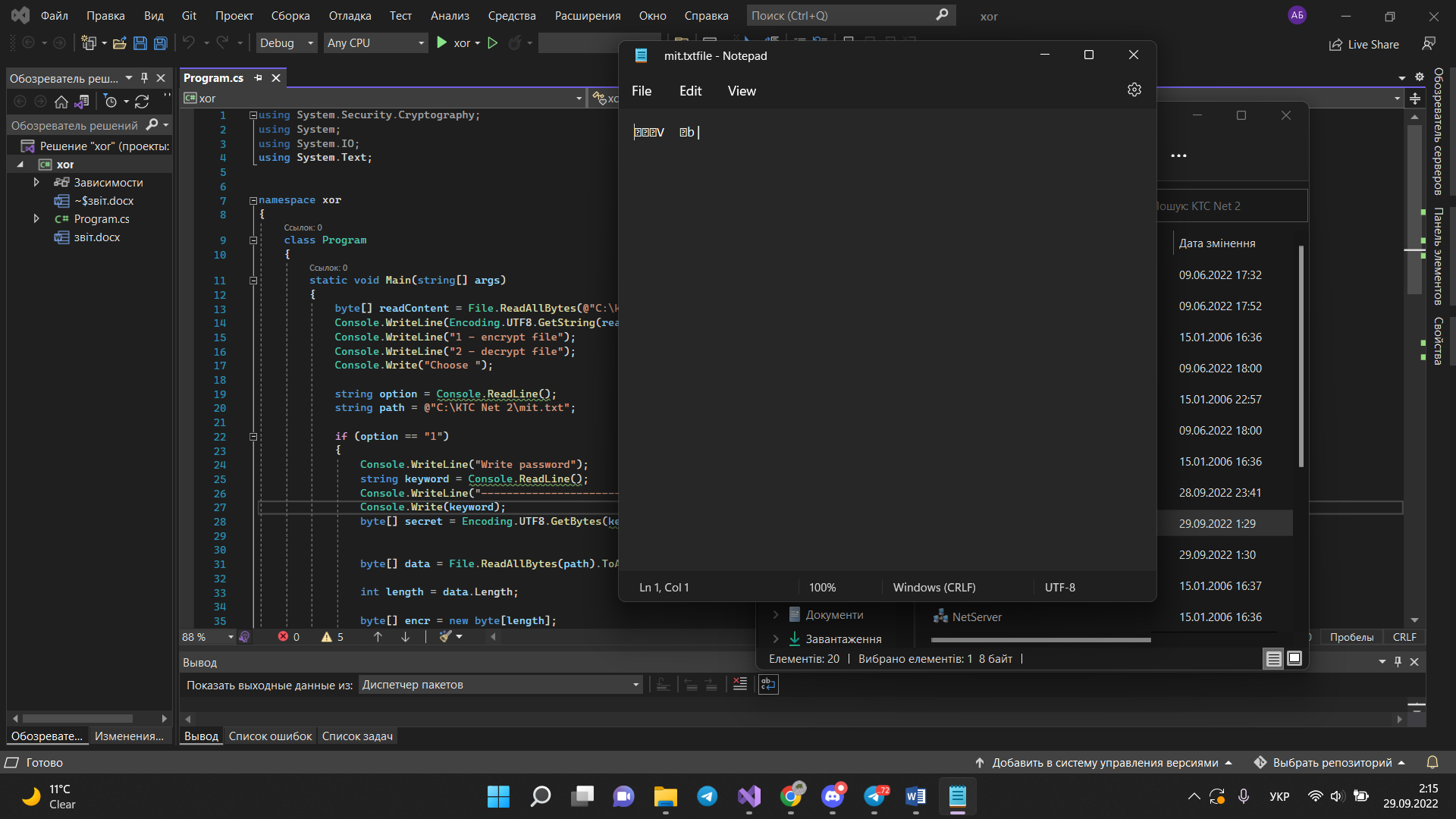
Завдання 1 Створити програму для зчитування файлу, шифрування його вмісту та запису зашифрованого фалу у ту ж саму папку але з розширенням \*.dat.

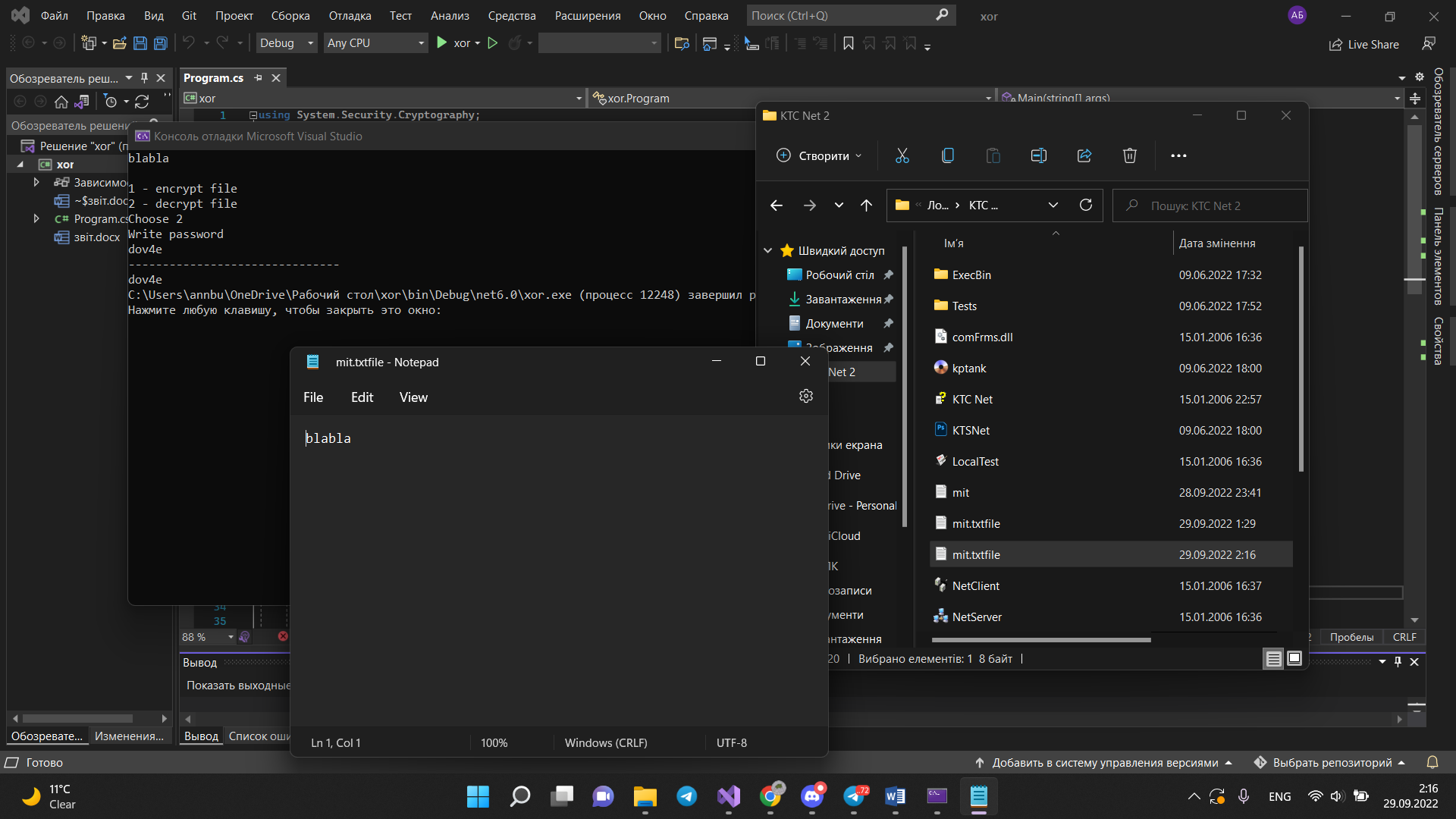
Завдання 2 Модифікувати програму так, щоб можна було розшифровувати зашифрований файл.

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.

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 його реалізовувати на С# і застосовувати для шифрування та розшифрування текстового файлу.