**Практичне заняття №2**

«Реалізація шифру Вернама»

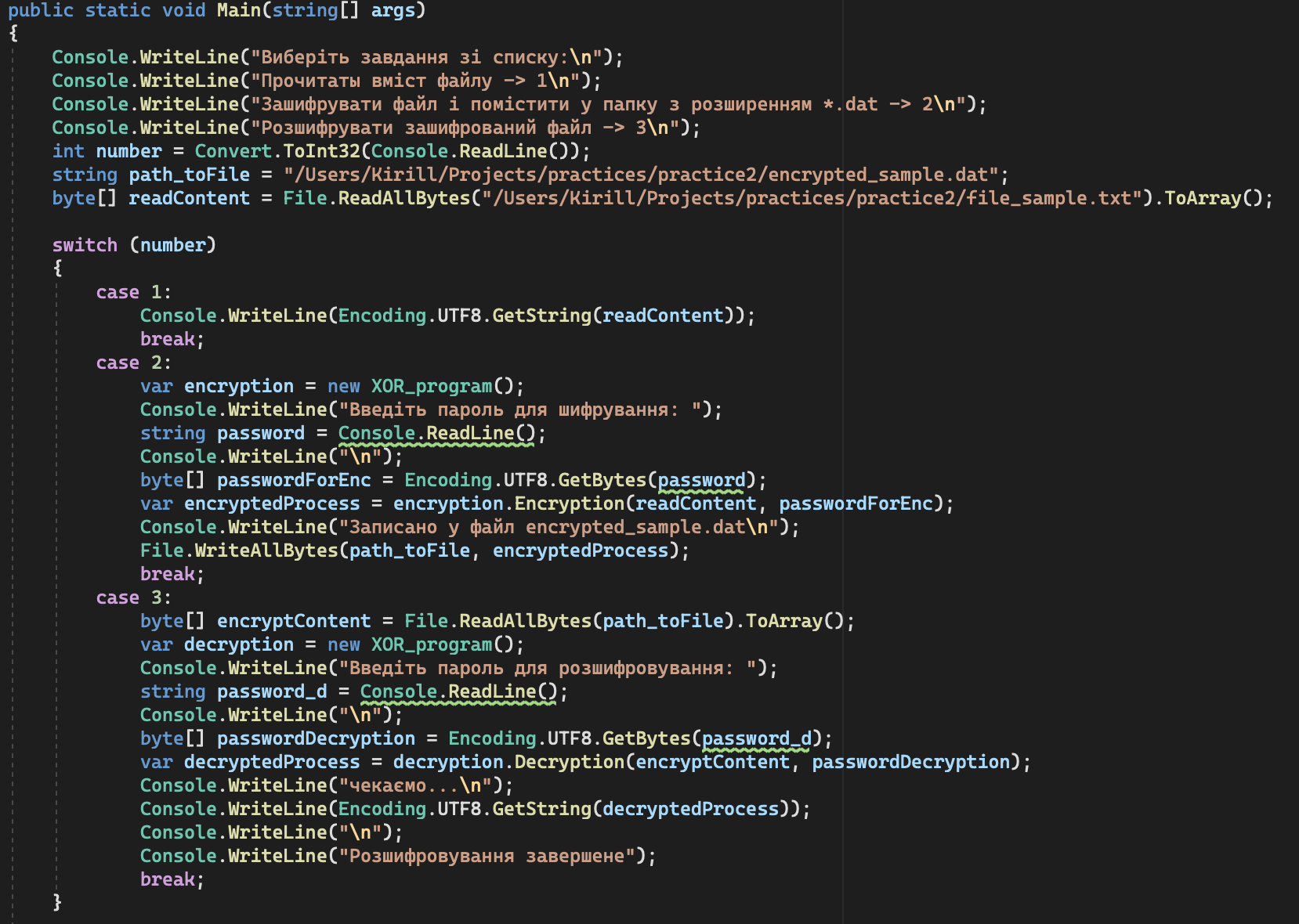
Виконав студент групи МІТ-21 Голомозик Кирила

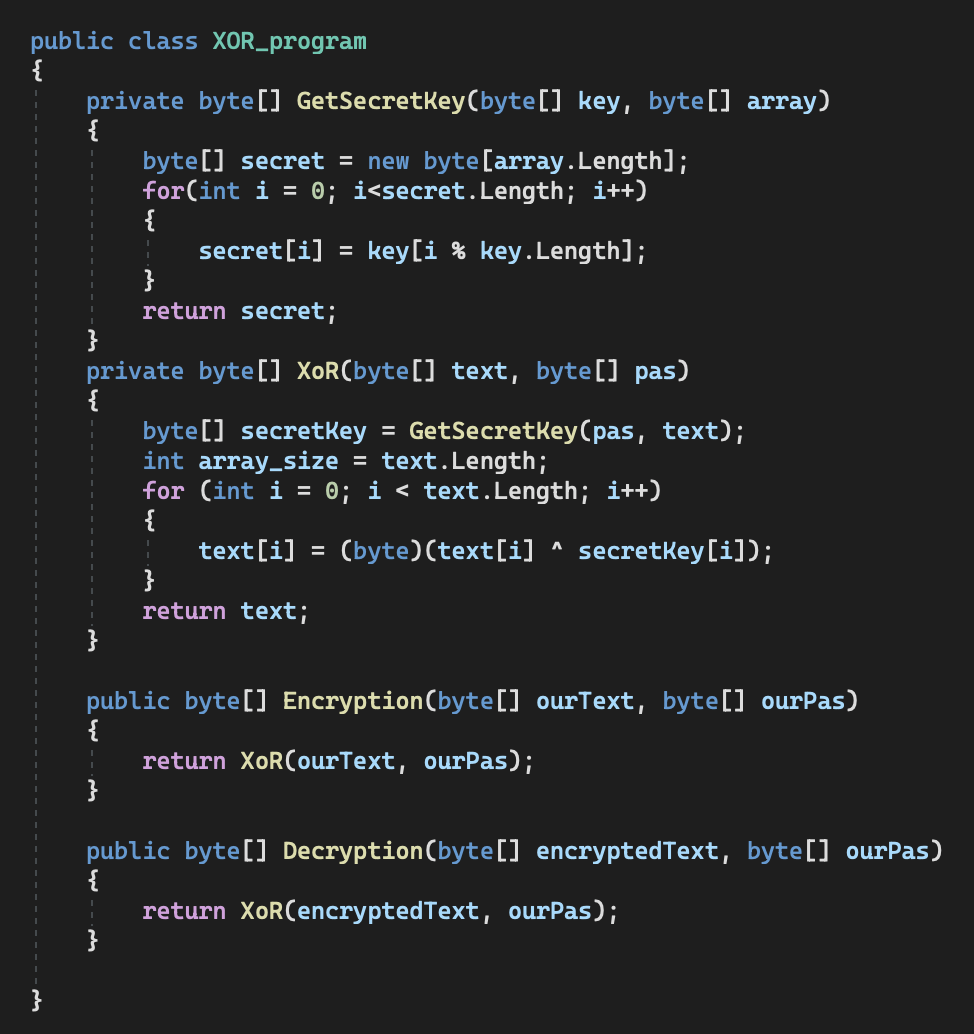
Мета: розібратися із шифром Вернама, розглянути операцію «виключне АБО» та написати програми для шифрування файлу даним шифром, його розшифрування та дешифрування.

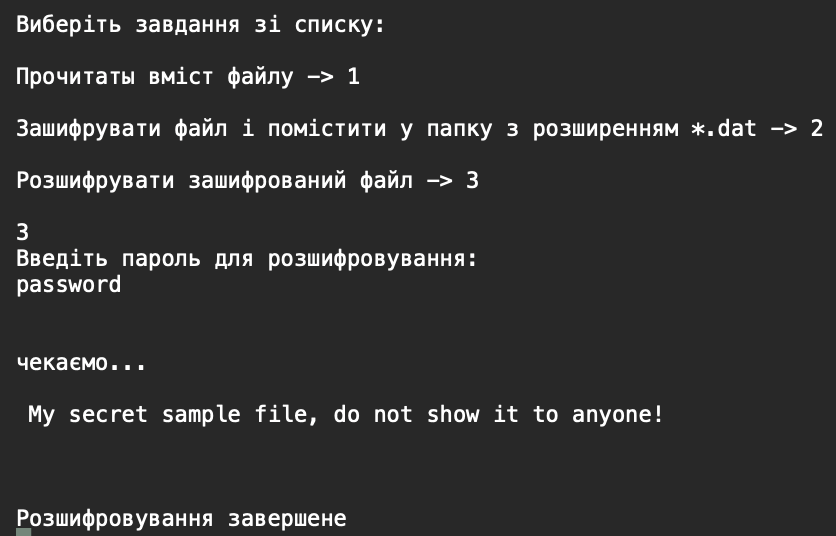
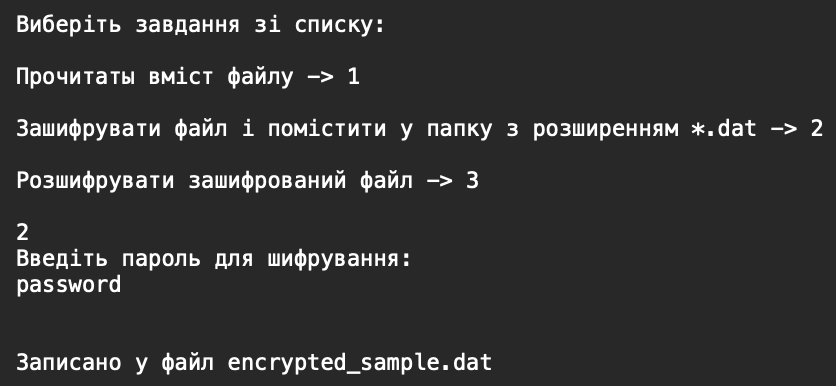
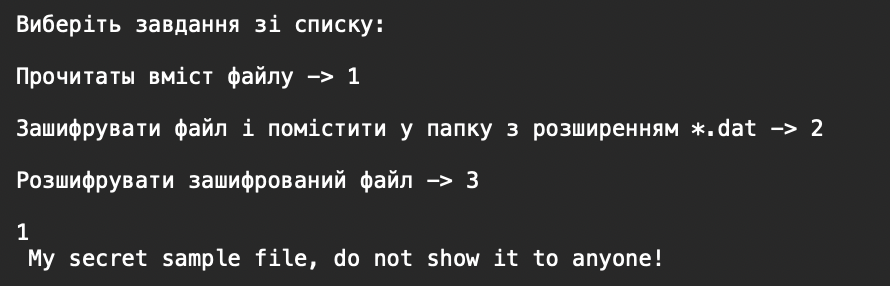
Хід роботи:

* 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 проекту підключимо простір імен System.Security.Cryptography, System.IO, System.Text і System.
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 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.
4. У разі розшифрування ми виконуємо ті ж самі дії, але замість мого файлу ми беремо наш новий зашифрований файл, а пароль використовуємо той самий.







Висновки: у ході практичного заняття були отримані вміння з написання програм для шифрування методом «виключне АБО» (шифром Вернама), вміння написати програми для розшифрування файлу і дешифрування невідомого нам файлу методом підбору паролей.