**Звіт**

**До практичної роботи**

**з дисципліни «Основи інформаційної безпеки»**

Студента Київського Національного Університету ім. Тараса Шевченко

Переверзева Олексія Сергійовича

Факультет інформаційних технологій

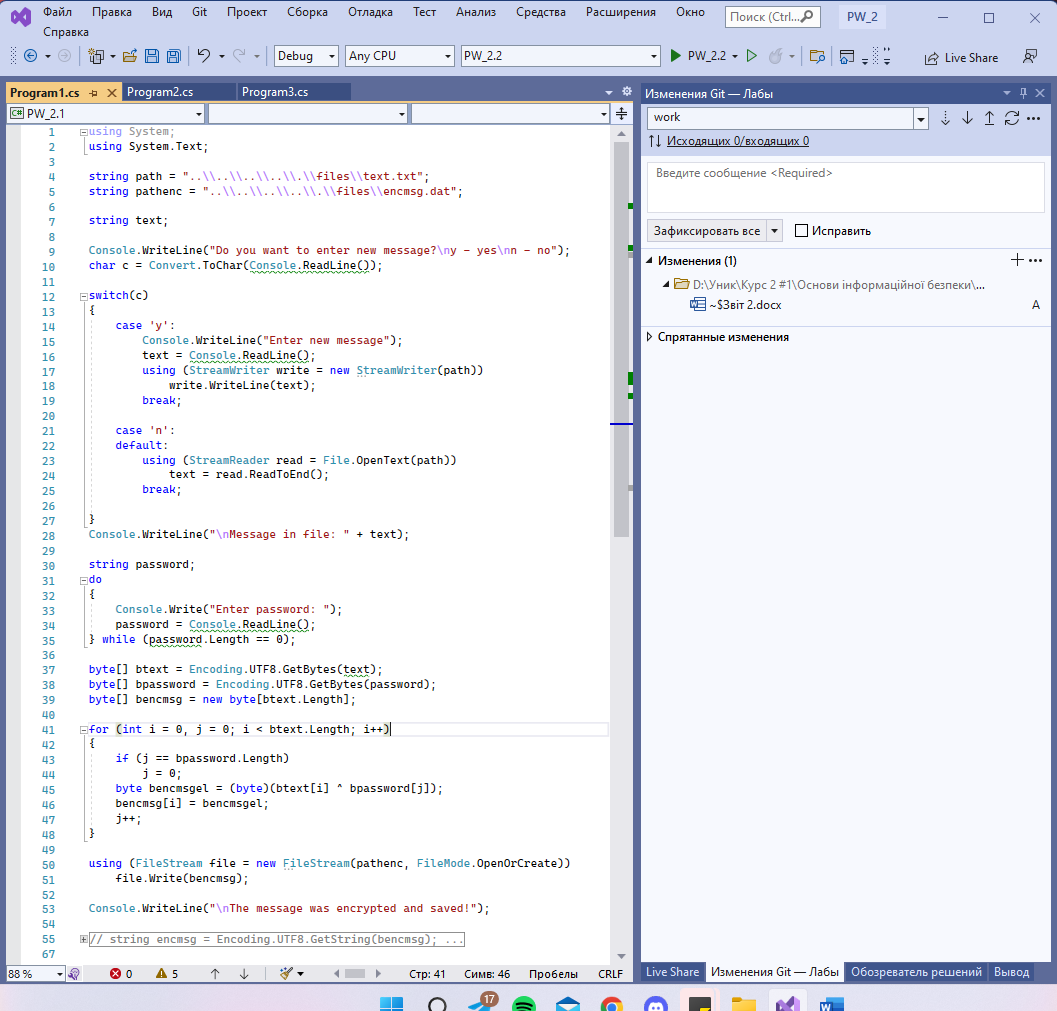
Група МІТ-21



**Практичне заняття №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 вкажемо шляхи до наших файлів:

string path = "..\\..\\..\\..\\.\\files\\text.txt";

string pathenc = "..\\..\\..\\..\\.\\files\\encmsg.dat";

Потім виконується запит на змінення вмісту файлу, можна змінити, так і залишити вміст файлу на поточний момент:

Console.WriteLine("Do you want to enter new message?\ny - yes\nn - no");

char c = Convert.ToChar(Console.ReadLine());

Відповідно за вибором користувача виконується один з двох варіантів:

* Змінити вміст файлу:

case 'y':

Console.WriteLine("Enter new message");

text = Console.ReadLine();

using (StreamWriter write = new StreamWriter(path))

write.WriteLine(text);

break;

Тобто виконується запит на введення нового тексту і він заміняє минулий вміст файлу

* Залишити вміст файлу:

case 'n':

default:

using (StreamReader read = File.OpenText(path))

text = read.ReadToEnd();

break;

Змінна string text буде зберігати або введений користувачем текст, або текст, зчитаний у файлі

Відповідно для зручності виводимо в консоль текст з файлу:

Console.WriteLine("\nMessage in file: " + text);

Далі вводимо нову змінну string password для зберігання ключа, який буде введеним користувачем, та відповідно виконуємо запит для введення цього ключа, який будемо використовувати для шифрування вмісту файлу:

do

{

Console.Write("Enter password: ");

password = Console.ReadLine();

} while (password.Length == 0);

Далі застосовуємо явне перетворення вміст файлу та введенного ключа:

byte[] btext = Encoding.UTF8.GetBytes(text);

byte[] bpassword = Encoding.UTF8.GetBytes(password);

Також нам потрібна змінна для запису результату операціїї XOR:

byte[] bencmsg = new byte[btext.Length];

Далі відповідно виконуємо XOR операцію, звертаючись до кожного елементу масива вмісту файлу та ключа:

for (int i = 0, j = 0; i < btext.Length; i++)

{

if (j == bpassword.Length)

j = 0;

byte bencmsgel = (byte)(btext[i] ^ bpassword[j]);

bencmsg[i] = bencmsgel;

j++;

}

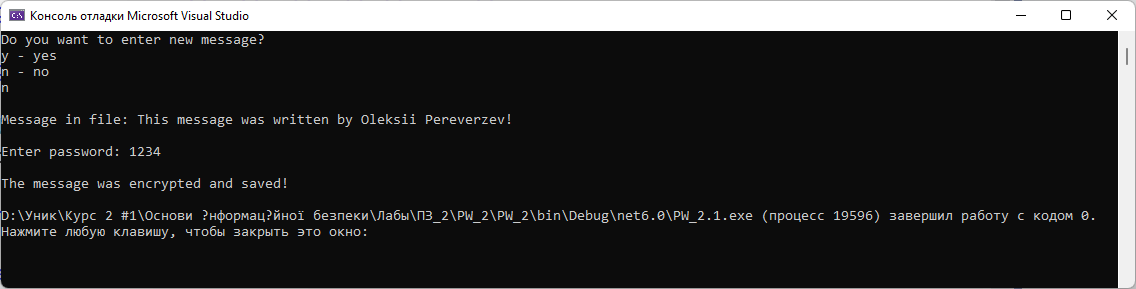
Якщо довжини ключа не вистачає, то, коли був використаний останній елемент масиву, починаємо використовувати його знову з початку.

Після завершення шифрування записуємо результат у файл с розширенням .dat:

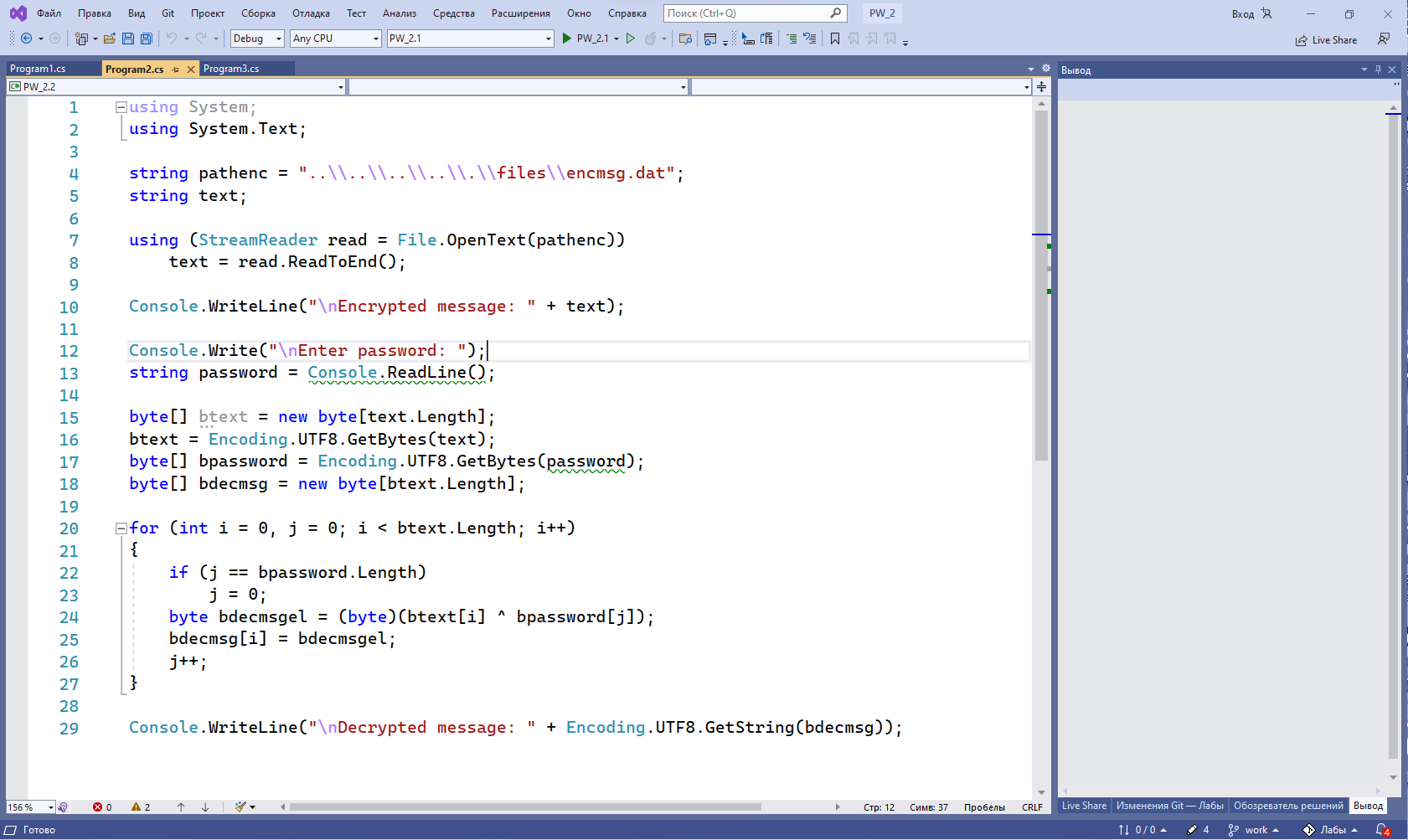
using (FileStream file = new FileStream(pathenc, FileMode.OpenOrCreate))

file.Write(bencmsg);

Виконання програми:



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



Розшифрування файлу виконав окремою програмою.

Так само відповідно вказуємо шлях до зашифрованого файлу, оголошуємо змінну для зберігання зчитаного вмісту файлу та зберігаємо його:

string pathenc = "..\\..\\..\\..\\.\\files\\encmsg.dat";

string text;

using (StreamReader read = File.OpenText(pathenc))

text = read.ReadToEnd();

Далі виконуємо запит на введення ключа, оголошуємо змінну та зберігаємо:

Console.Write("\nEnter password: ");

string password = Console.ReadLine();

Так само відповідно перетворюємо вміст ключа та файлу:

byte[] btext = new byte[text.Length];

btext = Encoding.UTF8.GetBytes(text);

byte[] bpassword = Encoding.UTF8.GetBytes(password);

і виконуємо розшифрування вмісту файлу:

for (int i = 0, j = 0; i < btext.Length; i++)

{

if (j == bpassword.Length)

j = 0;

byte bdecmsgel = (byte)(btext[i] ^ bpassword[j]);

bdecmsg[i] = bdecmsgel;

j++;

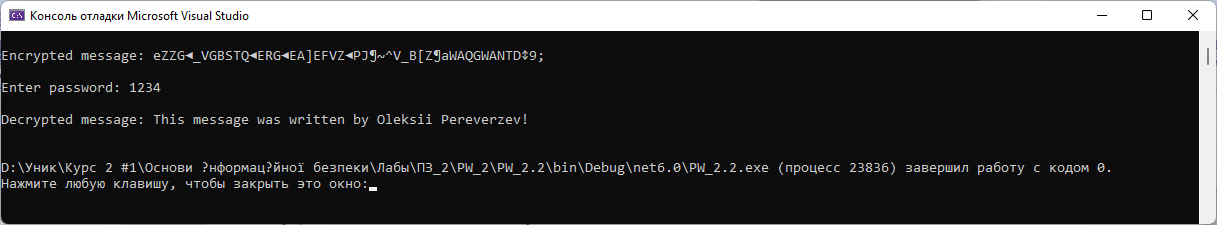
}

В кінці виводимо розшифрований вміст файлу, перетворивши його в текстове представлення:

Console.WriteLine("\nDecrypted message: " + Encoding.UTF8.GetString(bdecmsg));

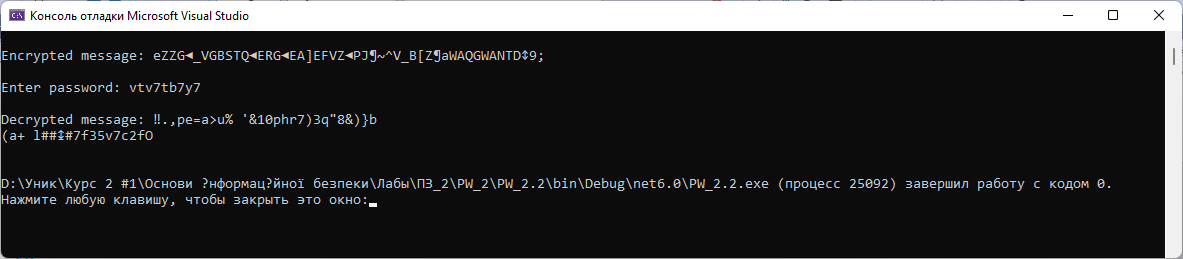
Виконання програми:

* При введенні правильного паролю:



Отримуємо в консолі відтворене повідомлення

* При введенні невірного паролю:



Отримуємо незрозумілий набір символів

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