

Міністерство освіти і науки України  
НТУУ «КПІ ім. Ігоря Сікорського»  
Навчально-науковий інститут атомної та теплової енергетики  
Кафедра цифрових технологій в енергетиці

Лабораторна робота №4  
з дисципліни «Безпека інформаційних систем»  
«Книжковий шифр»  
Варіант № 22

Виконав: Студент групи ТР-12  
Ковальов Олександр  
Перевірів: доцент, к.ф.-м.н.  
Тарнавський Ю. А.



## Фрагмент коду з реалізацією алгоритму шифрування/розшифрування.

```
public class LitFrag : SymmetricCipher
{
    private readonly List<char[]> _matrix;
    private readonly Dictionary<char, HashSet<string>> _dict;

    public LitFrag(string poem)
    {
        InitializeMatrix(poem, out _matrix);
        InitializeDictSet(_matrix, out _dict);
    }

    public override string Encrypt(string message, params object[] keys)
    {
        ValidateMessage(message.ToLower());

        var list = new List<string>();
        foreach (var c in message.ToLower())
        {
            var count = _dict[c].Count;
            list.Add(_dict[c].ElementAt(new Random().Next(count)));
        }

        return string.Join(", ", list);
    }

    public override string Decrypt(string message, params object[] keys)
    {
        ValidateEncryptedMessage(message);

        var sb = new StringBuilder();
        var list = message.Split(", ");

        foreach (var str in list)
        {
            var coords = str.Split("/");

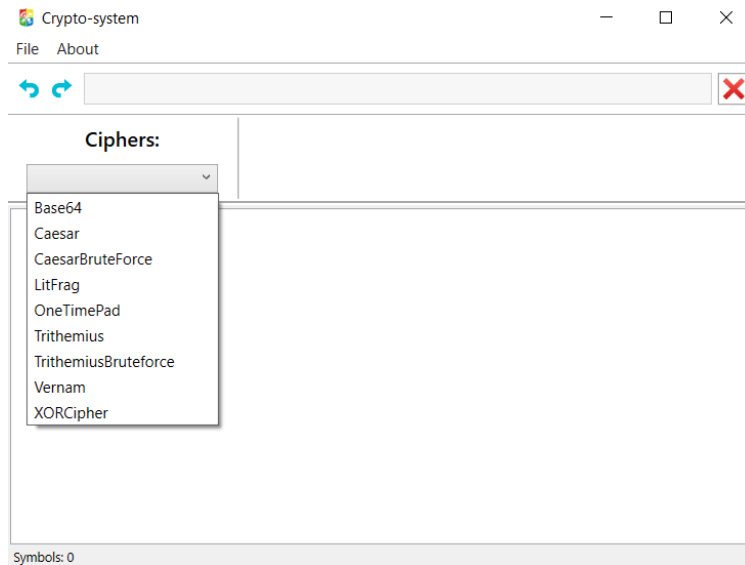
            // symbol position, format: line/position
            var l = int.Parse(coords[0]);
            var p = int.Parse(coords[1]);

            sb.Append(_matrix[l - 1][p - 1]);
        }

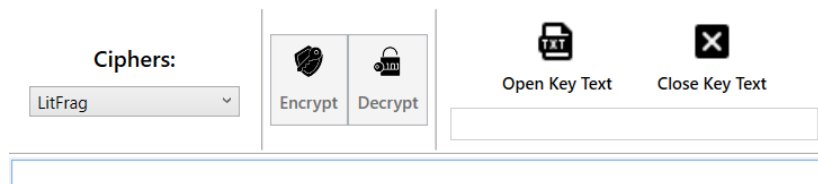
        return sb.ToString();
    }
}
```

## Скріншоти програми.

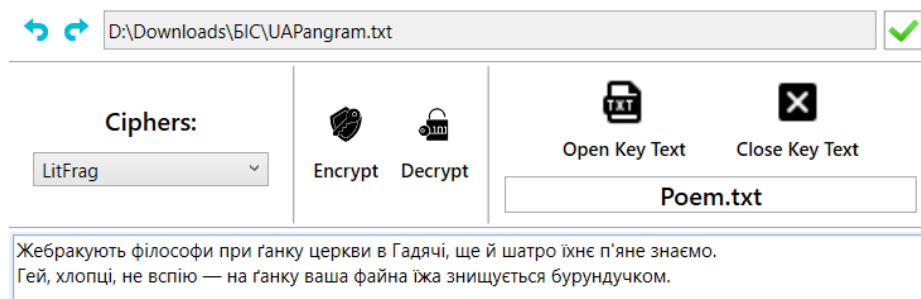
Головне вікно:



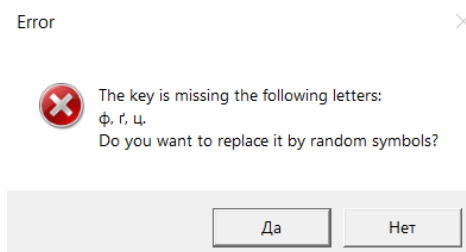
**Книжкове шифрування.** Є дві кнопки – шифрування та розшифрування. Також, є секція для завантаження ключа – літературного фрагменту.



Кнопки розблоковуються лише якщо в робочій області введений текст та в програму завантажений ключ:







Якщо в повідомленні є літери, яких немає у вірші, то виведеться повідомлення з питанням – чи можна підставити замість них випадкові?



## Результат шифрування:

Ciphers:  
LitFrag



 Encrypt  Decrypt



 Open Key Text  Close Key Text  
Poem.txt

11/10, 3/2, 23/6, 18/11, 1/18, 5/14, 3/11, 16/9, 23/10, 22/12, 7/5, 8/15, 20/11, 7/3, 14/2, 17/15, 16/12, 14/1, 15/4, 15/12, 20/10, 3/3, 12/14, 21/15, 15/11, 5/6, 2/6, 9/14, 13/10, 2/5, 6/13, 1/21, 3/15, 4/5, 22/20, 23/21, 21/15, 22/20, 16/10, 12/11, 14/14, 7/8, 23/17, 6/16, 11/21, 6/9, 21/9, 5/1, 13/3, 4/11, 17/7, 22/17, 3/13, 17/6, 15/5, 3/3, 10/10, 9/3, 4/8, 1/15, 7/9, 10/6, 16/5, 13/14, 23/16, 1/1, 9/6, 18/15, 17/10, 16/6, 9/18, 14/5, 10/6, 2/1, 3/20, 24/20, 19/21, 14/16, 14/13, 3/4, 4/16, 22/23, 4/3, 17/3, 24/15, 15/21, 3/10, 13/1, 12/1, 22/23, 19/2, 5/7, 1/21, 17/10, 4/4, 10/3, 13/14, 21/1, 19/13, 21/7, 12/16, 18/8, 12/5, 16/8, 23/12, 4/2, 12/4, 2/6, 19/15, 13/19, 9/3, 19/18, 4/7, 5/10, 17/17, 9/3, 8/15, 16/14, 1/19, 22/13, 17/17, 10/8, 4/8, 11/10, 16/14, 5/4, 19/10, 4/9, 7/7, 5/1, 10/1, 10/7, 1/10, 22/12, 3/1, 23/17, 1/3, 16/11, 7/2, 5/12, 10/1, 16/7, 23/8, 9/13, 7/18, 6/13, 1/11, 21/12, 15/11

## Результат розшифрування:

Ciphers:  
LitFrag



 Encrypt  Decrypt



 Open Key Text  Close Key Text  
Poem.txt

жебракують оілосоои при Панку 'еркви в гадЯчі, Ще й шатро їхНе п'Яне знаємо.  
гей, хлоп'ї, не всплю — На Панку ваша оайНа їжа зниЩується бурундучкоМ.

## Перед розшифруванням чи шифруванням текст проходить валідацію:


Ciphers:  
LitFrag

 Encrypt  Decrypt

 Open Key Text  Close Key Text  
Poem.txt

жебракують оілосоои пр  
гей, хлоп'ї, не всплю — Н

Error

 This text is not encrypted by LitFrag method.

OK

**Висновок:** за результатами виконання цієї лабораторної роботи було ознайомлено з принципом роботи шифрів, які використовують розподілений ключ. В крипто-систему був імплементований книжковий шифр. Шифр був частково покращений – зняте обмеження на «квадратність» матриці, масиви можуть бути «рваними». Також, на кожному кроці виконується валідація.