Національний технічний університет України

«Київський політехнічний інститут ім. Ігоря Сікорського»

Кафедра цифрових технологій в енергетиці

ЗВІТ   
з виконання лабораторної роботи №1  
з дисципліни «Безпека інформаційних систем»

«**Шифр Цезаря**»

Виконав: студент групи ТР-12 Каркушевський В.Л.

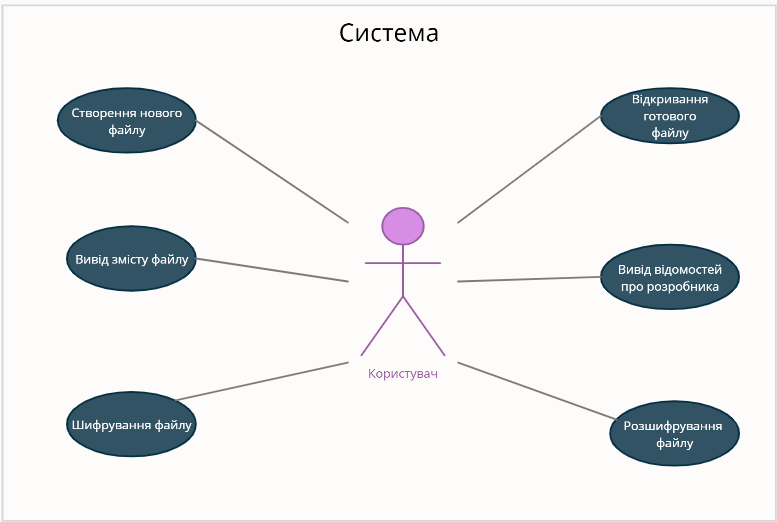
Перевірив: доцент, к.ф.-м.н.  
Тарнавський Ю.А.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

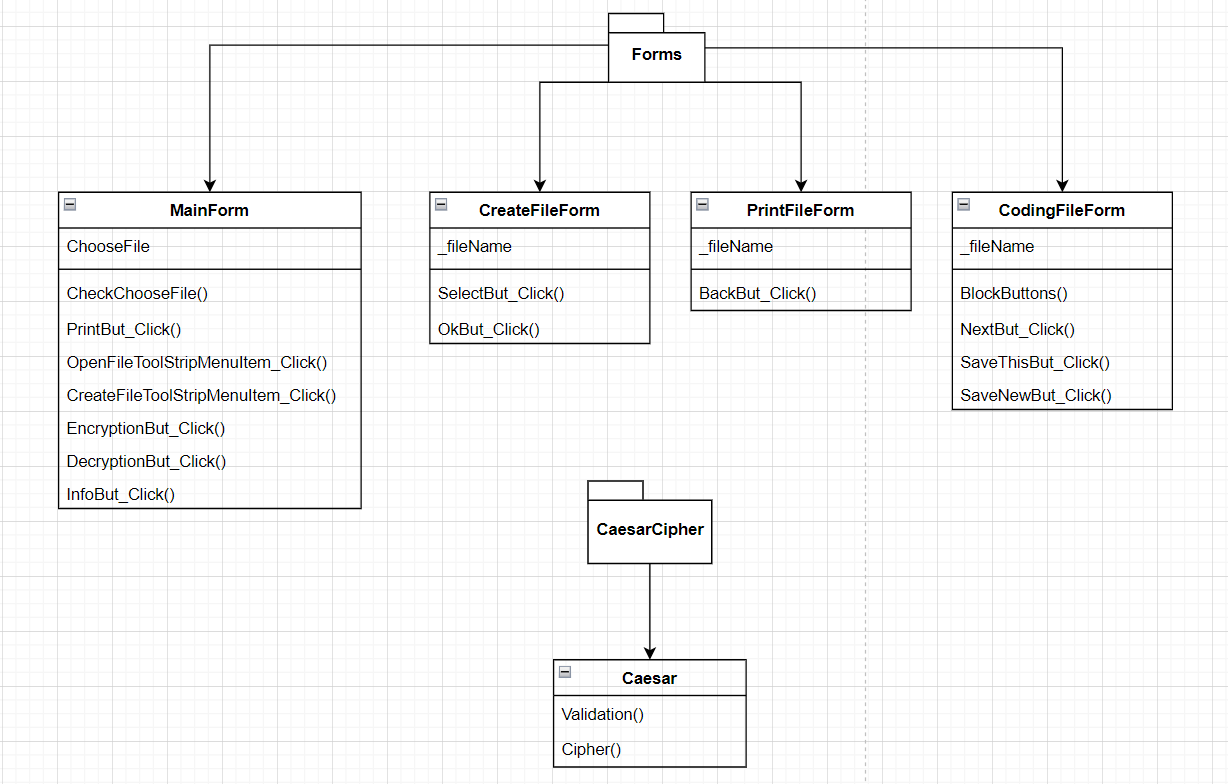
# **Мета роботи**

Розробити криптосистему на основі шифру Цезаря

# **Діаграма прецедентів**



# **Діаграма класів**



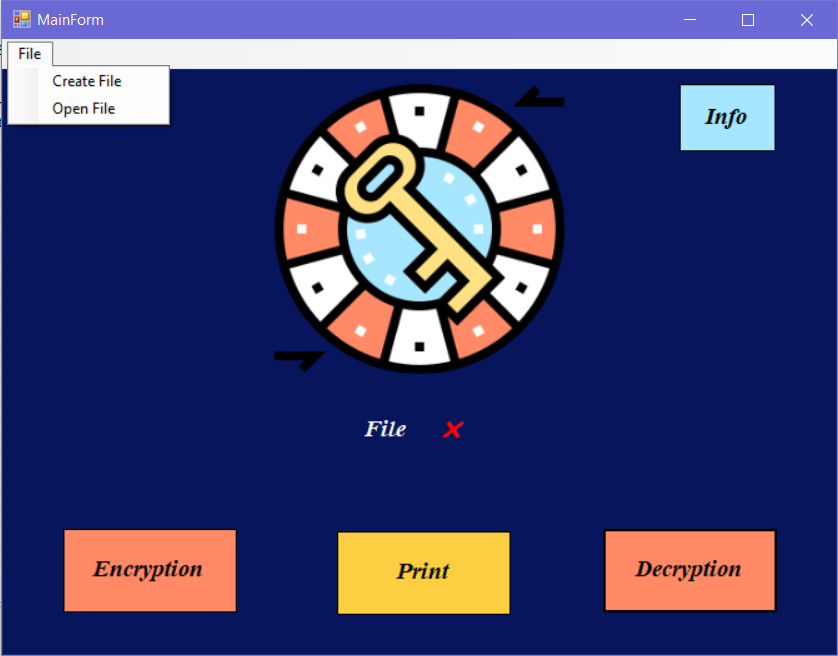
# **Фрагмент коду з реалізацією алгоритму шифрування/розшифрування**

private static bool *Validation*(char temp)  
 {  
 return temp != '?'**;** }  
  
 public static string *Cipher*(bool variant**,** string[] text)  
 **{** var sb = new StringBuilder()**;** var valid = 0**;** var windows1251 = Encoding.*GetEncoding*("windows-1251")**;** foreach (var line in text)  
 {  
 var encodedBytes = windows1251.GetBytes(line)**;** for (var j = 0**;** j < line.Length**;** j++)  
 {  
 if (encodedBytes[j] == 63)  
 {  
 if (*Validation*(line[j]))  
 {  
 if (valid == 0)  
 {

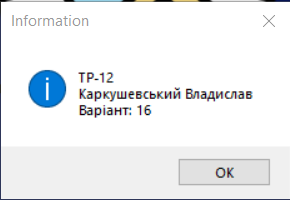
var a = MessageBox.*Show*(  
 @"The text contains an invalid symbol.   
The starting text can change after you confirm.  
Continue?"**,** @"Invalid symbol"**,** MessageBoxButtons.YesNo**,** MessageBoxIcon.Question**,** MessageBoxDefaultButton.Button1)**;** valid++**;** if (a == DialogResult.No)  
 {  
 return null**;** }  
 }  
 }  
 }  
  
 if (variant)  
 {  
 encodedBytes[j] += 5**;** }  
 else  
 {  
 encodedBytes[j] -= 5**;** }  
 }  
  
 sb.Append(windows1251.GetString(encodedBytes))**;** sb.AppendLine()**;** }  
  
  
 return sb.ToString()**;  
 }**

# **Скріншоти програми**

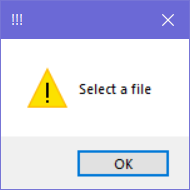
На початку роботи програми відкривається головна форма, у якій присутні кнопки з головними функціями



При натиску кнопки ‘Info’ відкривається вікно з інформацією про розробника



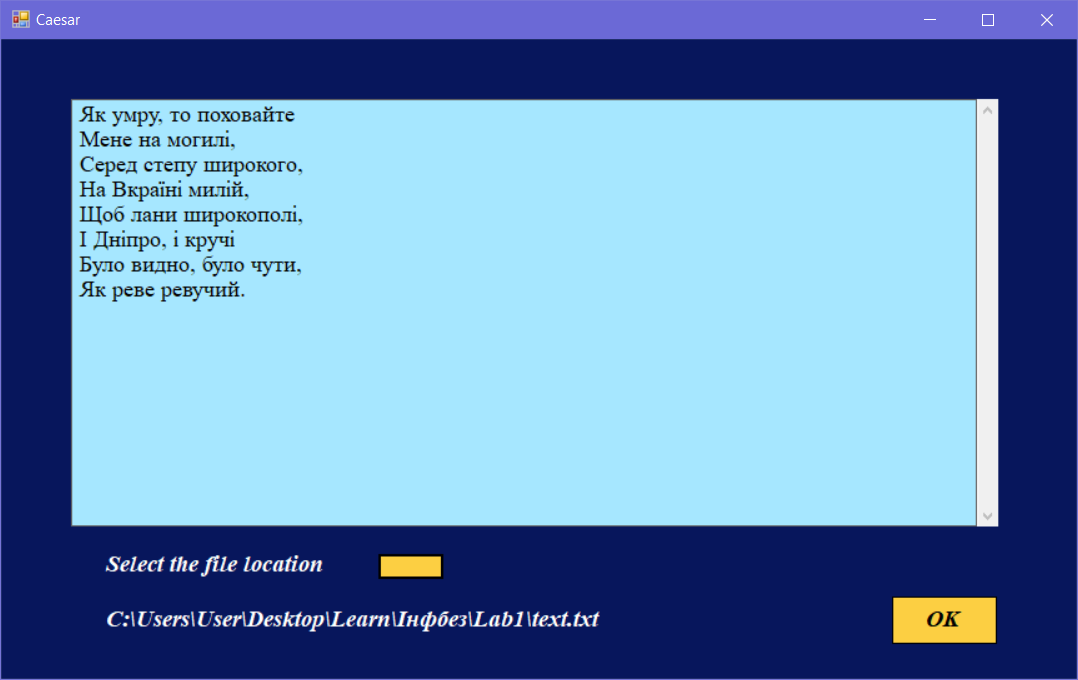
Для кодування/декодування потрібно обрати файл або створити новий. У випадку ігнорування цієї умови, і натисканні кнопок, у яких відбувається робота з файлом, виводиться попереджувальне повідомлення



При вибору пункту меню, для створення файлу відкривається нова форма, у якій потрібно ввести текст та обрати маршрут та назву файла



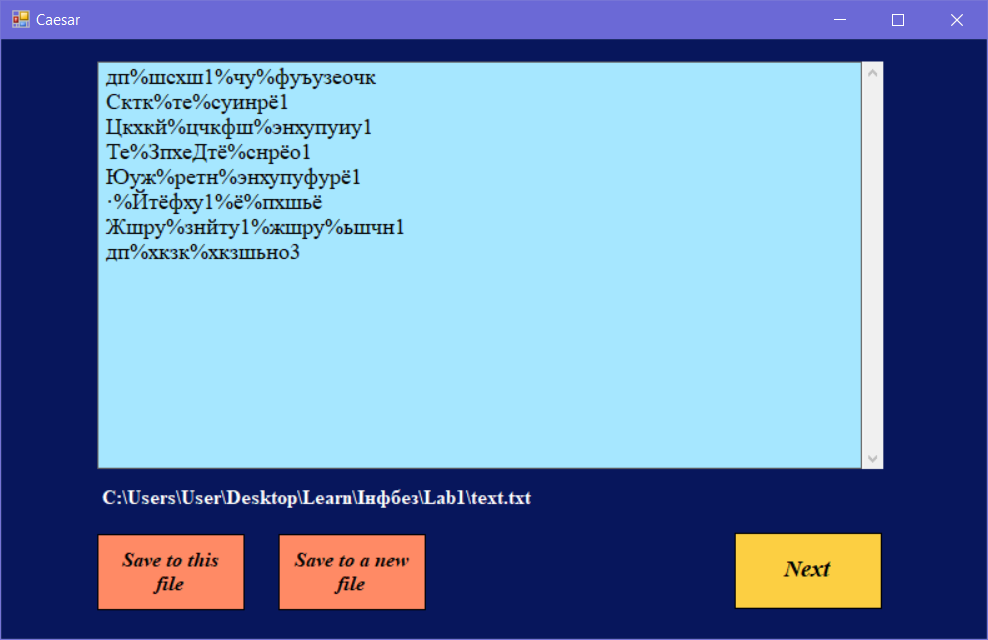
При недотриманні умов вводу тексту або вибору розташування файлу на екран виводяться відповідні повідомлення, у яких попереджається про виконання цих умов. У разі коректного введення тексту та обранні шляху файлу та при натиску кнопки ‘OK’ відбувається створення файлу у обраному місці та перенаправлення у головну форму.



Після обрання файлу на головній формі стають доступні функції кодування, декодування та виводу вмісту файлу. При натиску кнопки ‘Print’ відбувається перенаправлення у форму для виводу вмісту файлу.



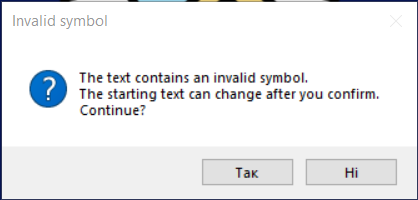
При натиску кнопки ‘Back’ відбувається повернення до головної форми. На головній формі, при натиску кнопки ‘Encryption’ відбувається шифрування тексту. Після цього виводиться вікно з повідомлення про успішне шифрування та відбувається перенаправлення у форму з результатом.



У цій формі присутні кнопки для збереження файлу у поточний файл та у новий. При вибору однієї з цих двох кнопок відбувається збереження у файл та блокується доступ для повторного збереження. При натиску кнопки ‘Next’ відбувається повернення до головної форми. На головній формі, при натиску кнопки ‘Decryption’ відбувається розшифрування тексту. Після цього виводиться вікно з повідомлення про успішне розшифрування та відбувається перенаправлення у форму з результатом.



Програма розрахована лише на кодування символів з набору ‘Windows-1251’. У випадку присутності у файлі символу який не входить до цього набору виводиться повідомлення, у якому представлений вибір наступних дій: продовження, з заміною некоректного символу на символ ‘D’ при кодуванні та символ ‘:’ при декодуванні, або ж припинення кодування.



# **Висновки**

На цій лабораторній роботі було ознайомлено з теоретичними відомостями про шифрування методом Цезаря. Розроблено програму з графічним інтерфейсом на мові програмування C# з використанням Windows Forms. У програмі реалізовано головні функції, такі як: створення, відкривання, збереження, друкування, шифрування, розшифрування файлів та виведення відомостей про розробника. Виконано тестування роботи шифрування та розшифрування.