Національний технічний університет України

«Київський політехнічний інститут ім. Ігоря Сікорського»

Кафедра цифрових технологій в енергетиці

ЗВІТ   
з виконання лабораторної роботи №7  
з дисципліни «Безпека інформаційних систем»

«**Шифрування з відкритим ключем на основі алгоритму RSA**»

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

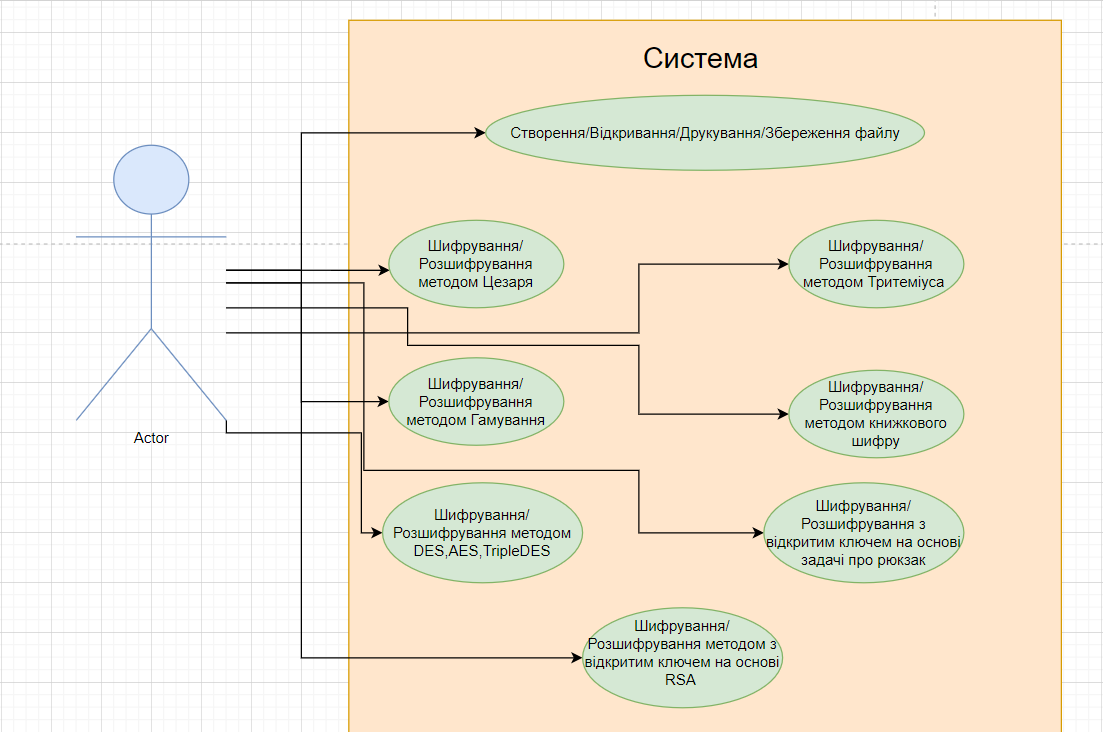
Перевірив: доцент, к.ф.-м.н.  
Тарнавський Ю.А.

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

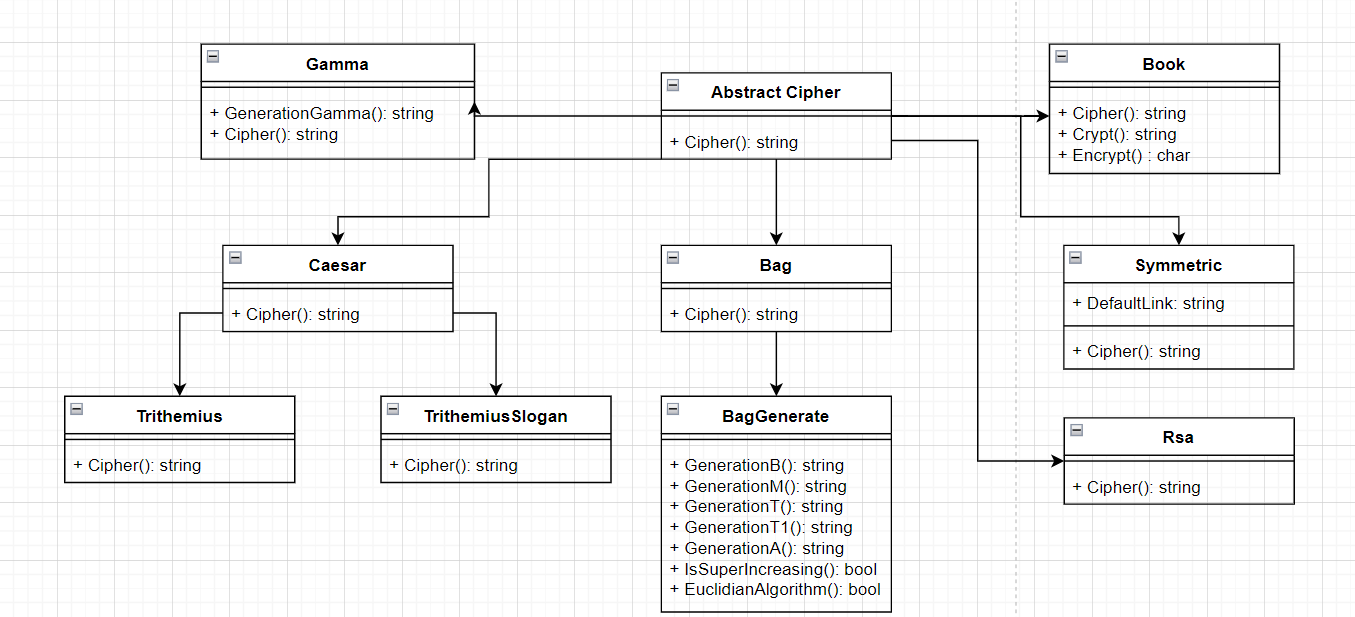
# **Мета роботи**

Ознайомитись з використанням криптопровайдерів .Net для побудови асиметричної криптосистеми

# **Діаграма прецедентів**



# **Діаграма класів**



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

**AbstractCipher**

public abstract class AbstractCipher  
**{** protected const int AlphabetSize = 55295**;** // кількість символів в алфавіті Unicode  
   
 public abstract string Cipher(bool variant**,** string[] text**,** string startKey)**;**}

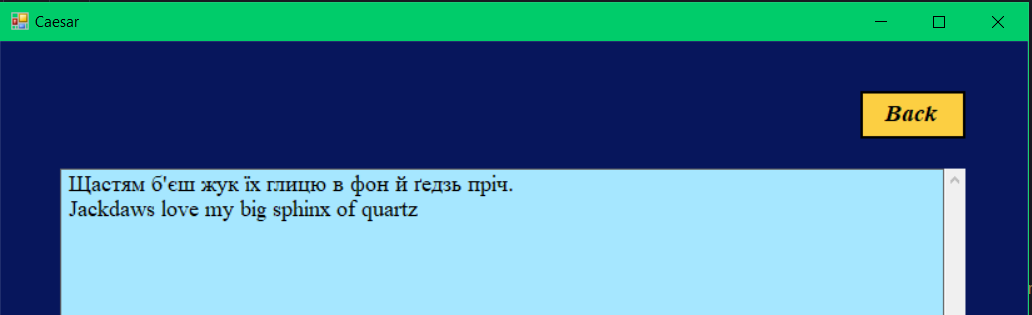
public class Symmetric : AbstractCipher  
**{**

**Rsa**

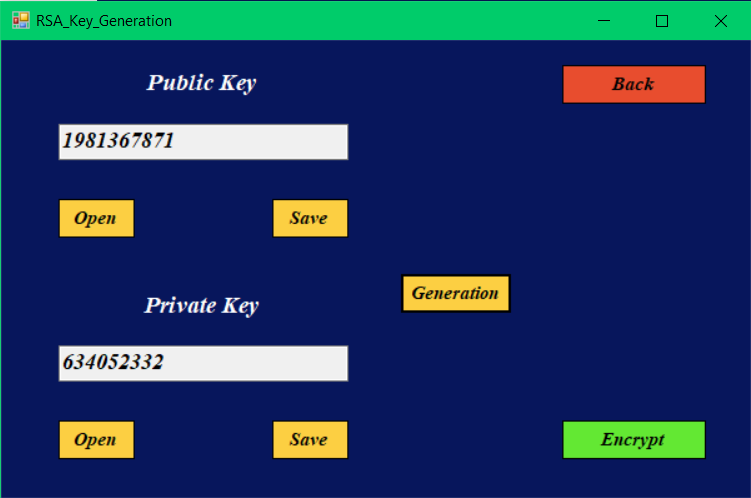
public class Rsa : AbstractCipher  
{  
 public override string Cipher(bool variant**,** string[] text**,** string[] startKey)  
 **{** var rsa = new RSACryptoServiceProvider()**;** rsa.FromXmlString(startKey[0])**;** var res = new StringBuilder()**;** foreach (var lineOfText in text)  
 {  
 if (variant)  
 {  
 var byteToEncrypt = Encoding.Unicode.GetBytes(lineOfText)**;** var encryptBytes = rsa.Encrypt(byteToEncrypt**,** false)**;** res.Append(string.*Join*(" "**,** encryptBytes.Select(b => b.ToString())))**;** }  
 else  
 {  
 var encryptBytes = lineOfText.Split(' ').Select(byte.*Parse*).ToArray()**;** var decryptBytes = rsa.Decrypt(encryptBytes**,** false)**;** res.Append(Encoding.Unicode.GetString(decryptBytes))**;** }  
  
 res.AppendLine()**;** }  
  
  
 return res.ToString()**;** }

# **Скріншоти програми**

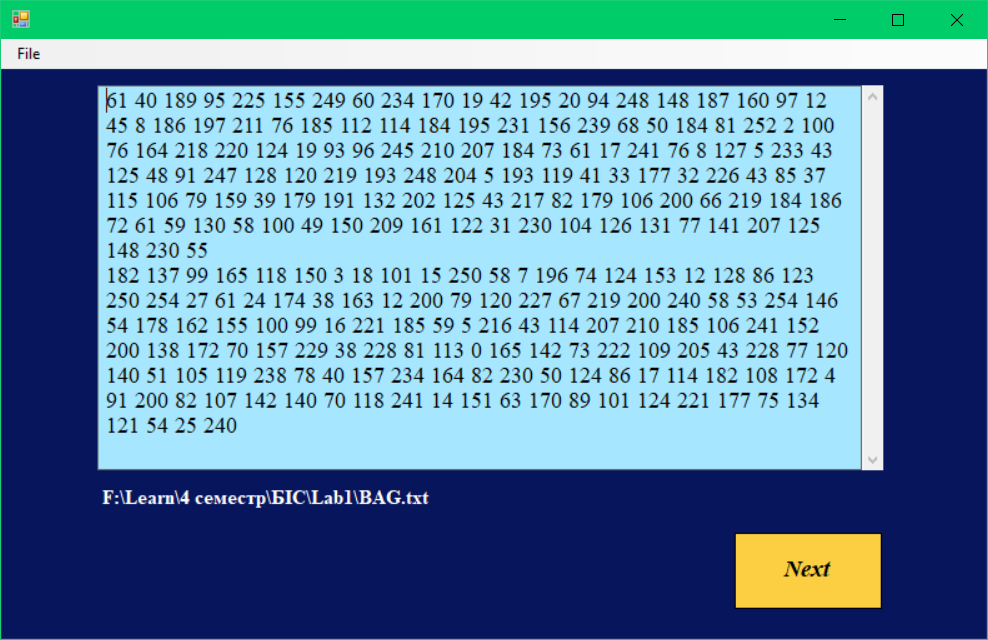
Оберемо панграму



Оберемо метод шифрування з відкритим ключем на основі задачі RSA та натиснемо encryption. В результаті відбувається перехід на наступну форму. Згенеруємо ключі та збережемо їх у файли.



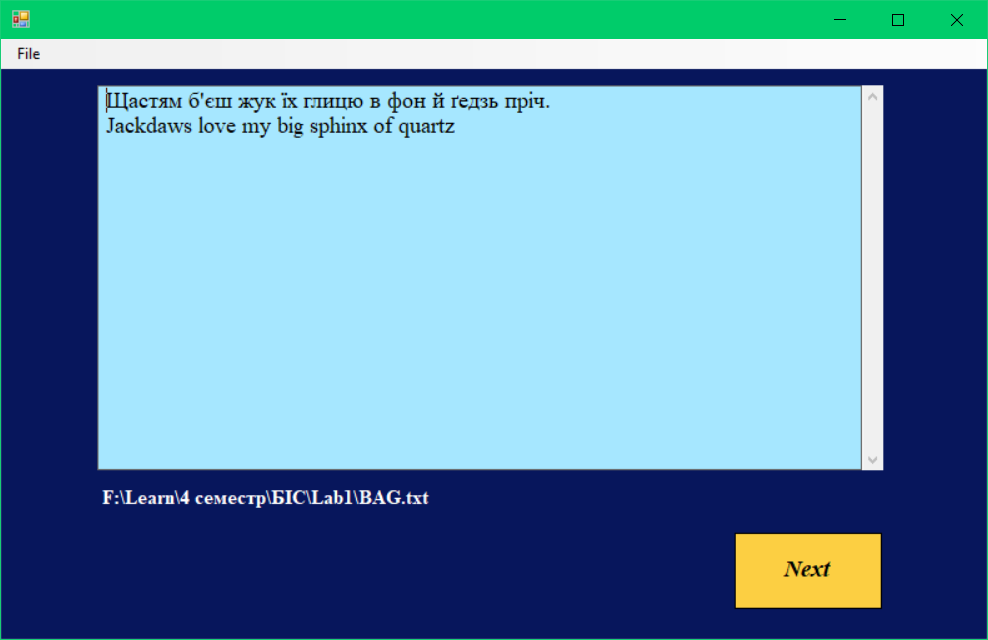
Зашифруємо текст. У результаті отримуємо



Збережемо результат. Для розшифрування натиснемо decrypt. В результаті відбувається перехід на наступну форму. Відкриваємо приватний ключ для розшифрування та натискаємо Decrypt



Розшифруємо текст. У результаті отримуємо



# **Висновки**

На цій лабораторній роботі було ознайомлено з теоретичними відомостями з використанням криптопровайдерів .Net для побудови асиметричної криптосистеми. Модифіковано програму, розроблену у 6 лабораторній роботі, з графічним інтерфейсом на мові програмування C# з використанням Windows Forms. У програму доповнено новий метод шифрування з відкритим ключем на основі алгоритму RSA. Виконано тестування роботи шифрування та розшифрування.