МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

**Звіт із**

**Теорія імовірності та математичної статистики**

**Лабораторна робота №3**

з курсу «Математичні основи криптології»

Виконав:

Готюк Максим

Група Пмі-33

Оцінка \_\_\_

2025

Тема: Шифр Гамування

Мета: Розробити криптосистему на основі шифру гамування

**Постановка завдання:**

1. Адаптуйте інтерфейс криптографічної системи симетричного

шифрування з лабораторної роботи №1 або №2 для реалізації

шифрування методом гамування.

1. Доповніть систему класів з попередніх лабораторних робіт класами

та методами, необхідними для:

* 1. генерації гами, період якої перевищує довжину вхідного тексту;
  2. реалізації симетричного шифрування методом гамування.

1. Виконайте тестування роботи системи.
2. Модифікуйте розроблену систему, забезпечивши можливість

шифрування і розшифрування за допомогою шифроблокноту, як це

передбачено в шифрі Вернама.

## **Програмна реалізація**

Для розробки інтерфейсу веб-застосунку я скористався мовою C# та фреймворком ASP.NET Core MVC 9.0.

Додана можливість обрати шифр Гамування.

A screen shot of a computer

AI-generated content may be incorrect.

Доступна можливіть енкрипції та декрипції з циклічним ключем або шифроблокнотом.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Для кожного файлу доступні частотні таблиці:  
A screenshot of a computer

AI-generated content may be incorrect.

**Тестування системи:**Написані такі Юніт тести:

**A screen shot of a computer

AI-generated content may be incorrect.**

**Пояснення тестів:**

* **Тести для EncryptAsync:**
* **EncryptAsync\_WithOneTimePad\_ReturnsCorrectEncryptedText: Перевіряє, що метод EncryptAsync повертає правильний зашифрований текст при використанні одноразового шифроблокноту.**
* **EncryptAsync\_WithGamma\_ReturnsCorrectEncryptedText: Перевіряє, що метод EncryptAsync повертає правильний зашифрований текст при використанні гами.**
* **EncryptAsync\_ThrowsException\_WhenLanguageNotSupported: Перевіряє, що метод EncryptAsync викидає виняток, якщо мова не підтримується.**
* **Тести для DecryptAsync:**
* **DecryptAsync\_WithOneTimePad\_ReturnsCorrectDecryptedText: Перевіряє, що метод DecryptAsync повертає правильний розшифрований текст при використанні одноразового шифроблокноту.**
* **DecryptAsync\_WithGamma\_ReturnsCorrectDecryptedText: Перевіряє, що метод DecryptAsync повертає правильний розшифрований текст при використанні гами.**
* **DecryptAsync\_ThrowsException\_WhenLanguageNotSupported: Перевіряє, що метод DecryptAsync викидає виняток, якщо мова не підтримується.**
* **Тести для GenerateOneTimePad:**
* **GenerateOneTimePad\_ReturnsCorrectLength: Перевіряє, що метод GenerateOneTimePad повертає одноразовий шифроблокнот правильної довжини.**
* **GenerateOneTimePad\_ThrowsException\_WhenLanguageNotSupported: Перевіряє, що метод GenerateOneTimePad викидає виняток, якщо мова не підтримується.**
* **Тести для GetBinaryIndices:**
* **GetBinaryIndices\_ReturnsCorrectBinaryRepresentation: Перевіряє, що метод GetBinaryIndices повертає правильне двійкове представлення індексів алфавіту.**
* **GetBinaryIndices\_ThrowsException\_WhenLanguageNotSupported: Перевіряє, що метод GetBinaryIndices викидає виняток, якщо мова не підтримується.**
* **Тести для GetBinaryTextRepresentation:**
* **GetBinaryTextRepresentation\_ReturnsCorrectBinaryRepresentation: Перевіряє, що метод GetBinaryTextRepresentation повертає правильне двійкове представлення тексту.**
* **GetBinaryTextRepresentation\_ThrowsException\_WhenLanguageNotSupported: Перевіряє, що метод GetBinaryTextRepresentation викидає виняток, якщо мова не підтримується.**
* **Тести для GetEncryptionProcess:**
* **GetEncryptionProcess\_ReturnsCorrectProcessDescription: Перевіряє, що метод GetEncryptionProcess повертає правильний опис процесу шифрування.**
* **GetEncryptionProcess\_ThrowsException\_WhenLanguageNotSupported: Перевіряє, що метод GetEncryptionProcess викидає виняток, якщо мова не підтримується.**

**Ці тести охоплюють основні функціональності XORCipherService і забезпечують правильну поведінку сервісу в різних сценаріях.  
  
Висновок**  
У ході виконання лабораторної роботи було розроблено криптографічну систему на основі шифру Гамування, яка підтримує шифрування та розшифрування текстових українською та англійською мовами. Система включає інтерфейс для зручного управління файлами, функції шифрування/розшифрування, активну, а також побудову частотних таблиць для аналізу текстів.