Звіт  
По Практичному заняттю номер 2  
З основ інформаційної безпеки  
Студента Ларіонова Володимира  
  
Використовуючи методи з System.Security.Cryptography можна згенерувати криптографічно стійкий одноразовий ключ, який можна використовувати для шифрування повідомлення шифром Вернама. Шифр Вернама має один недолік, а саме можливість дешифровки повідомлення, якщо один і той самий ключ використовується декілька разів.   
Для шифрування повідомлення методами .NET ми перетворюємо вхідне повідомлення у масив байтів та генеруємо ключ для шифрування. Потім для кожного байту повідомлення та ключа використовуємо операцію XOR. Отриманий під кінець масив байтів є зашифрованим повідомленням. Для розшифрування повідомлення потрібно застосувати до нього та використаного для шифрування ключа ту ж саму операцію XOR.  
  
Висновки:  
Шифр Вернама не є абсолютно надійним, якщо один і той самий ключ використовується більше ніж один раз, або якщо довжина ключа менша за довжину повідомлення (при шифруванні ключ повторюється). Для шифрування у C# потрібно виконати операцію XOR окремо для кожного байту повідомлення та ключа (наприклад, за допомогою циклу for та масивів байтів, що представляють собою вхідне повідомлення та ключ)  
  
Github-репозиторій:

<https://github.com/LoUyyR12/Information-Security.git>