Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет інформатики та обчислювальної техніки

Кафедра інформатики програмної інженерії

Основи захисту інформації

Лабораторна робота № 2

Тема: Bad nonce

**Виконав:**

Студент гр. ІТ-82

Фолькін Д. О.

**Перевірив:**

ст. вик. Ісаченко Г. В.

Оцінка:\_\_\_\_\_\_\_\_\_\_\_

(\_\_)\_\_\_\_\_\_\_\_\_\_2021

Київ – 2021

**Хід роботи**

Задача: маємо надійний потоковий шифр Salsa20, у якому не використовують nonce і не змінюють ключ. Необхідно розшифрувати текст.

Потокові шифри, у яких ключ використовується кілька разів для різних повідомлень вразливий до атак що спрямовані на використання вразливості повтору ключа та на особливість операції XOR.

Ми застосуємо обидві техніки.

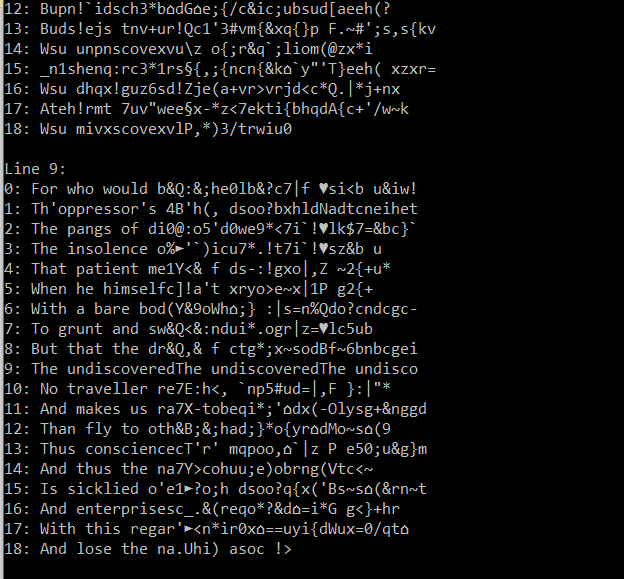
Напишемо просту програму на С#.

Алгоритм такий – ми вводимо початкове слово, яке з високою вірогідністю зустрічатиметься у тексті. Робимо XOR кожного рядка з кожним, отримуємо результати, результати XOR-имо з рядком і отримуємо набір текстів, один з яких точно буде мати нові зрозумілі мовні одиниці. Зберігаємо такий фрагмент і використовуємо його для розширення пошуку, себто збільшуємо довжину нашого слова. Коли ми досягнемо певної довжини – ми розв’яжемо усю задачу цілком.

Підбираємо наші рядки, наприклад почнемо із «The» (можна використовувати будь-які слова, ще хорошим кандидатом може бути with, when, and, for…).

Поступово розкриваючи нові і нові фрагменти, можемо встановити і весь рядок.

Приклад роботи (вводимо черговий фрагмент «The undiscovered»):



Врешті решт можемо логічно здогадатися яке слово може доповнювати конструкцію, або здійснити пошук фрагмента або рядка в інтернеті. Це суттєво звужує коло пошуку.

У результаті підбору маємо фрагмент з «Гамлету», автор - Вільям Шекспір.

For who would bear the whips and scorns of time,  
Th' oppressor's wrong, the pround man's contumely,  
The pangs of despis'd love, the law's delay,  
The insolence of office, and the spurns  
That patient merit of th' unworthy takes,  
When he himself might his quietus make  
With a bare bodkin; who would fardels bear,  
To grunt and sweat under a weary life,  
But that the dread of something after death,  
The undiscover'd country, from whose bourn  
No traveller returns, puzzles the will,  
And makes us rather bear those ills we have,  
Than fly to others that we know not of?  
Thus conscience does make cowards of us all,  
And thus the native hue of resolution  
Is sicklied o'er with the pale cast of thought,  
And enterprises of great pitch and moment  
With this regard their currents turn awry,  
And lose the name of action