Потокові шифри – симетричні шифри, де біти текста комбінуються з потоком бітів згенерованих псевдорандомним генератором за допомогою xor операції (тому що ця операція не відображає інформацію про зашифрований текст та є оберненою до самої себе).

Такі шифри вразливі до атак якщо один і той самий ключ без nonce використаний більш ніж один раз.

Наприклад повідомлення A і B і потоковий шифр згенерував C(K) бітів.

Тоді зашифровані версії повідомлень:

E(A) = A xor C

E(B) = B xor C

Якщо ми обрахуємо

E(A) xor E(B) = (A xor C) xor (B xor C) = A xor B xor C xor C = A xor B

То отримаємо шифр, який є шифром Віженера з ключем, який дорівнює довжині меншого з повідомлень. Такий шифр можна було б вважати теоретично незламним якби не те, що обидва повідомлення не є випадковою послідовністю символів, а природною мовою.

У цій лабораторній кожен рядок зашифрований за допомогою одного й того ж ключа без nonce. Для влому можна використати метод crib dragging:

1. Підібрати два повідомлення
2. Вибрати слово, яке може міститись в одному з цих повідомлень (найбільш ймовірно, що це буде одне з найбільш вживаних слів, тому для збільшення шансу краще використати одне з них).
3. З вибраного слова отримати масив байтів
4. Отримати два масива байтів з обраних на кроці 1 повідомлень, виконати над ними операцію xor.
5. Виконати операцію xor над масивами байтів, отриманими на кроці 3 (вибране слово) та 4, при цьому, якщо масив байтів вибраного слова менший за повідомлення, то краще конкатенувати його з самим собою допоки довжина отриманого масиву не буде дорівнювати довжині масиву повідомлення.
6. Якщо текст, отриманий з попереднього кроку не є читабельним, алгоритм повторюється починаючи з кроку 2.

Вгадавши одне зі слів, ми можемо додавати до цього слова інший текст, який на нашу думку може бути там присутнім, таким чином розшифровуються обидва повідомлення (одне буде складатись з відгаданих нами слів, другу – зі слів отриманих в результаті виконання алгоритму). Варто зазначити, що таким чином ми можемо розшифрувати обидва повідомлення, але не дізнатися яке з повідомлень який текст містить.

Для взлому використовувався:

<https://lzutao.github.io/cribdrag/>

Джерела:

1. <https://en.wikipedia.org/wiki/Stream_cipher_attacks>
2. <https://crypto.stackexchange.com/questions/59/taking-advantage-of-one-time-pad-key-reuse>
3. <http://travisdazell.blogspot.com/2012/11/many-time-pad-attack-crib-drag.html>