Потокові шифри вразливі до атак, якщо один і той же ключ використовується два або більше разів.

Припустимо, ми надсилаємо повідомлення *A* і *B* однакової довжини, обидва зашифровані за допомогою одного ключа *K*. Нехай потоковий шифр видає рядок бітів *C (K)* такої ж довжини, що і повідомлення. Тоді зашифрованими версіями повідомлень є:

E (A) = A ***xor*** *C*

E (B) = B ***xor*** *C,*

де ***xor*** виконується побітно.

Операція ***xor*** є комутативною і має властивість *X* ***xor*** *X = 0*, звідси:

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

Іншими словами, якщо хтось перехоплює два повідомлення, зашифровані одним і тим же ключем, він може відновити *A* ***xor*** *B*.

Для таких випадків існує метод, який називається **crib dragging**, що може розкрити звичайний текст двох повідомлень, зашифрованих одним і тим же ключем, навіть не знаючи ключа.

Алгоритм розшифровки повідомлення за допомогою **crib dragging** приблизно наступний:

1. Підбирається слово, яке може з'явитися в одному з повідомлень – «*crib-слово»*.
2. Зі слова з кроку 1 отримується масив байт (також можлива реалізація з hex рядками).
3. Виконується операція ***xor*** над масивами байт, що були отримані з двох зашифрованих повідомлень (*E (A)* ***xor*** *E (B)*).
4. Виконується операція ***xor*** над масивами з кроків 3 та 2.
5. Масив байт, отриманий на кроці 4, переводиться у рядок.
6. Якщо результат з кроку 5 є читабельним текстом, ми вгадуємо англійське слово та розширюємо наш пошук, переходячи до кроку 1 з новим отриманим *«crib-словом»*.
7. Якщо результат не є читабельним текстом, ми пробуємо виконати крок 4, зсуваючись по масиву з кроку 3 на наступну позицію.
8. Якщо ми пройшлися по масиву з кроку 3 до кінця і так і не натрапили на читабельний текст, переходимо на крок 1 і підбираємо нове «*crib-слово»*.

Існують готові реалізації **crib dragging** калькуляторів, які були використані для виконання даної лабораторної роботи, наприклад:

- https://toolbox.lotusfa.com/crib_drag/
- https://lzutao.github.io/cribdrag/

Якщо вихідні зашифровані повідомлення різної довжини, довше повідомлення «обрізається» до розміру коротшого. Так атака виявить лише ту частину довшого повідомлення, яку покриває коротше. Але це не завадить розшифрувати «покриту» частину тим же методом.