Якщо використовувати один і той самий ключ то у мене для вас погані новини.   
Бо зловмисник знає що ми надіслали 2 повідомлення і зробити XOR кожного з одним ключем. Тобто теоретично зловмисник ( тобто я ) може зробити наступне

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

А і В – початкові повідомлення

Використання одного у того самого ключа дозволяє зробити **crib dragging .** Тільки от шо то такое треба знати. Ви знаєте? Ніт?! Капець. Тоді я розкажу:

Crib Dragging це спосіб розшифрування повідомлень. Алгоритм приблизно такий:

1. Підбирається слово, яке може з’явитися в одному з повідомлень – «crib-слово».

А як його ж взнати? Ну я керувалась логікою що там зашифрований англійський текст, залізла у Гугль і знайшла яке слово зустрічається найчастіше.

1. Зі слова з кроку 1 отримується масив байт (або hex рядки).
2. Виконується операція **xor** над масивами байт, що були отримані з двох зашифрованих повідомлень (E (A) **xor** E (B)).
3. Виконується операція **xor** над масивами з кроків 3 та 2 та переводиться у рядок
4. Якщо результат з кроку 4 є схоже на текст, БІНГО слово вгадане та розширює пошук. Тут треба знову зробити крок 1 з новим отриманим «crib-словом».
5. Якщо результат не є читабельним текстом, ми пробуємо виконати крок 3, зсуваючись по масиву з кроку 2 на наступну позицію або міняємо слово або розуміємо що треба ще брати рядки і **xor**ити.

І ось так поки не розшифруємо все. Я використовувала онлайн калькулятор для цього.

А що ж робити якщо повідомлення різної довжини? Треба зробити їх однієї і орієнтуємось на довжину коротшого. Так атака виявить лише ту частину довгого повідомлення, яку покриває коротше. Але це не завадить розшифрувати «покриту» частину тим же методом.

