Звіт лабораторна №2

Для виконання другої лабораторної роботи використовувався Crib Drag Calculator.

Знаючи те, що для шифрування кожного рядку поеми використовувався один і той же ключ, без використання солі, ми можемо його дешифрувати за допомогою Crib Drag method навіть не знаючи ключа.

Це відбувається за наступним алгоритмом:

Для шифрування ми використовуємо One time pad, довжина якого дорівнює довжині ключа.

PlainText1 XOR RandomKey = CipherText1

PlainText2 XOR RandomKey = CipherText2

При існуванні тільки одного ключа ми можемо здійснити наступну операцію:

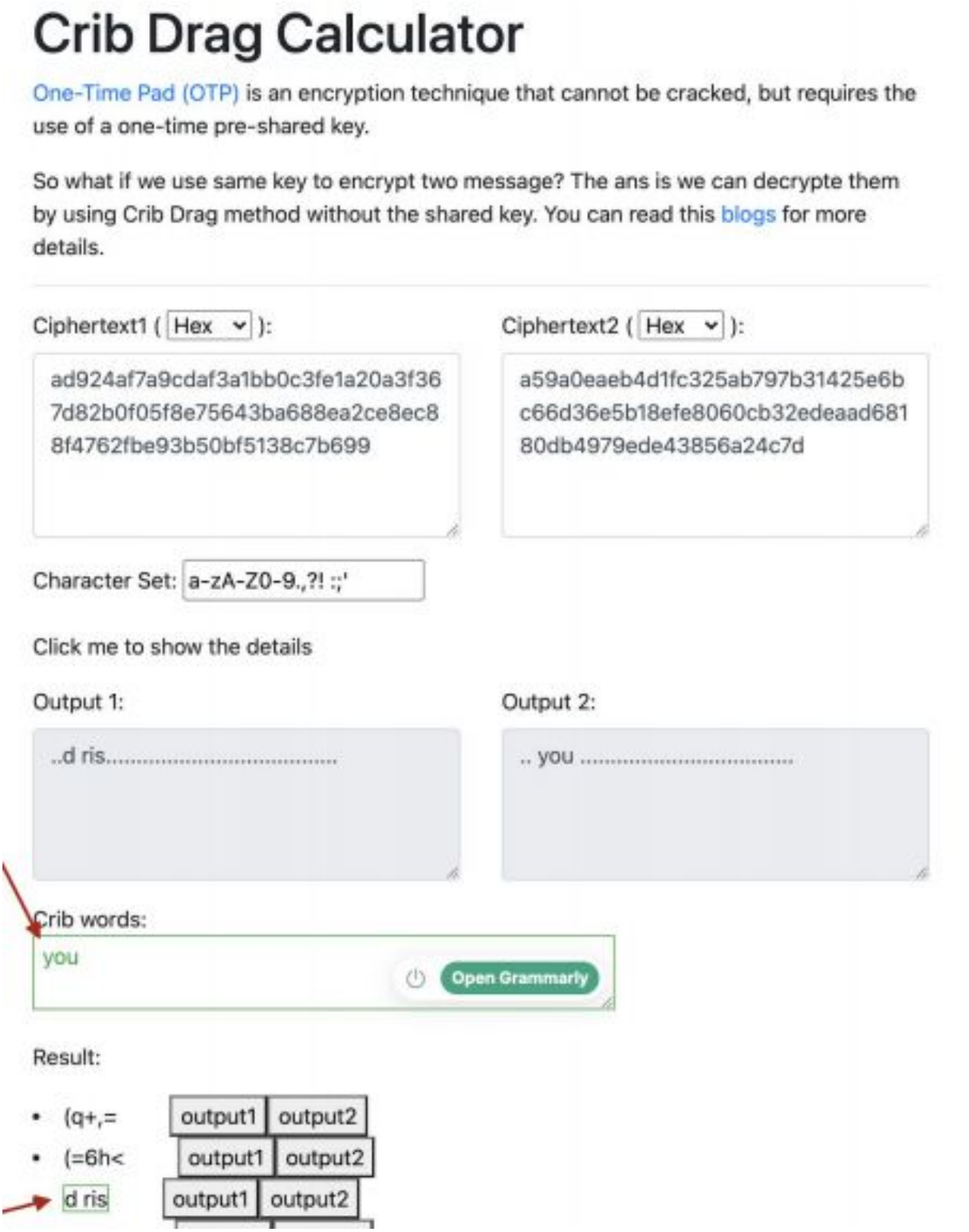
CipherText1 XOR CipherText2 = (PlainText1 XOR RandomKey) XOR (PlainText2 XOR RandomKey)) = PlainText1 XOR PlainText2

Таким чином ми можемо відгадуючи частини слів в першому повідомленні, ми автоматично відгадуємо частину, яка знаходиться на тій ж позиції в другому повідомленні.

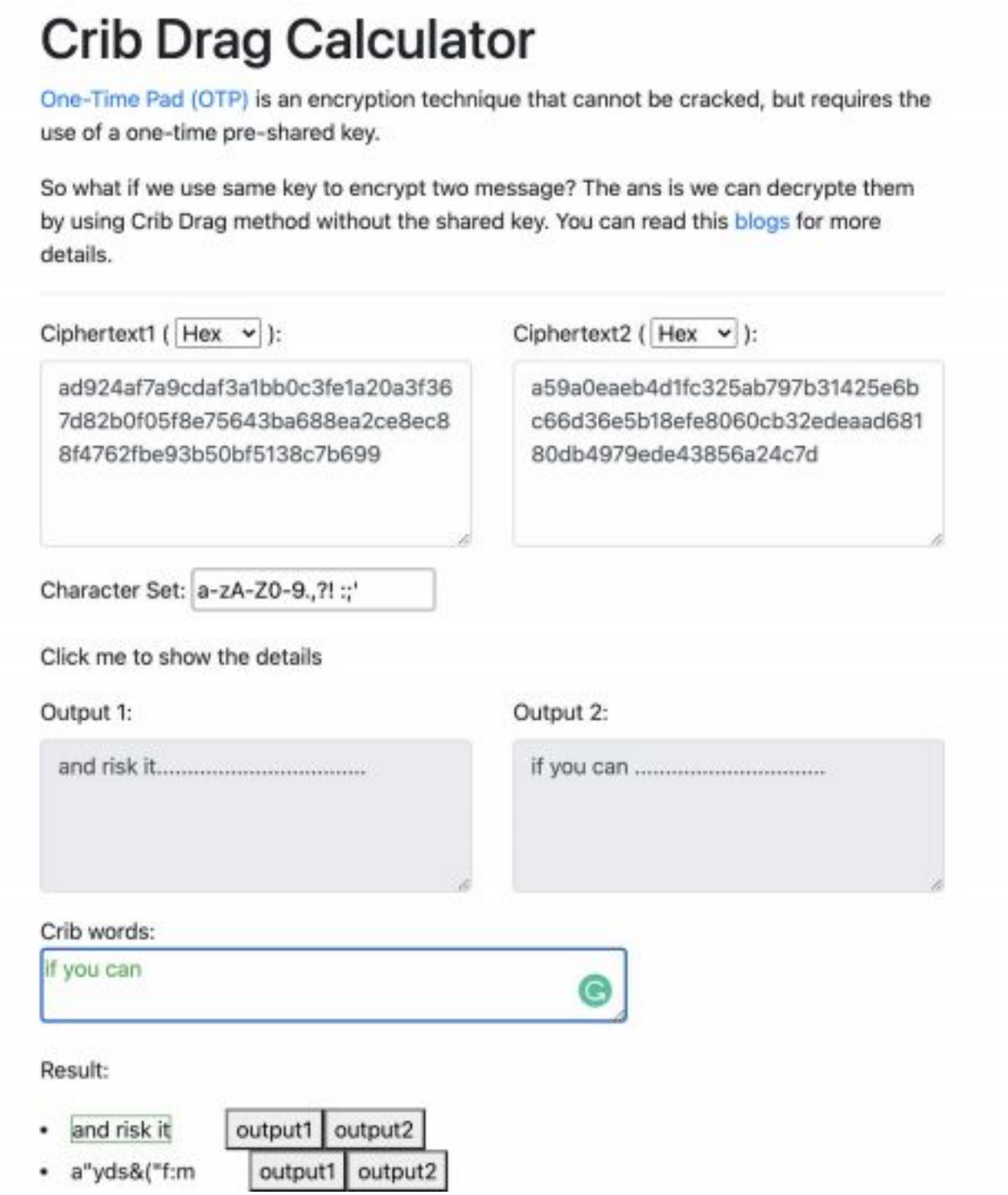
За допомогою Crib Drag Calculator пробуємо підбирати слова, які можуть зустрітися в зашифрованому тексті. Для вибору слів можна використати список Сводеша для Англійської мови

https://geo.koltyrin.ru/spisok_svodesha.php?jazyk=english.

Після кількох невдалих спроб вдалося знайти частинку оригінального тексту. Для цього було використано слово you(з пробілами навколо)



Далі перебором слів довжиною 3, що закінчуються на символ “d” було знайдено наступні частини поеми “if you” “and ris”. Продовжуючи такий ж перебір було знайдено “if you can” та “and risk it”, чого було вже достатньо для пошуку даної поеми.



Автор даної поеми - Редьярд Кіплінг та назва поеми “if”.

Отже, навіть безпечний алгоритм такий як Salsa20 може бути зламаним, якщо використовувати один і той же ключ для шифрування різних повідомлень.