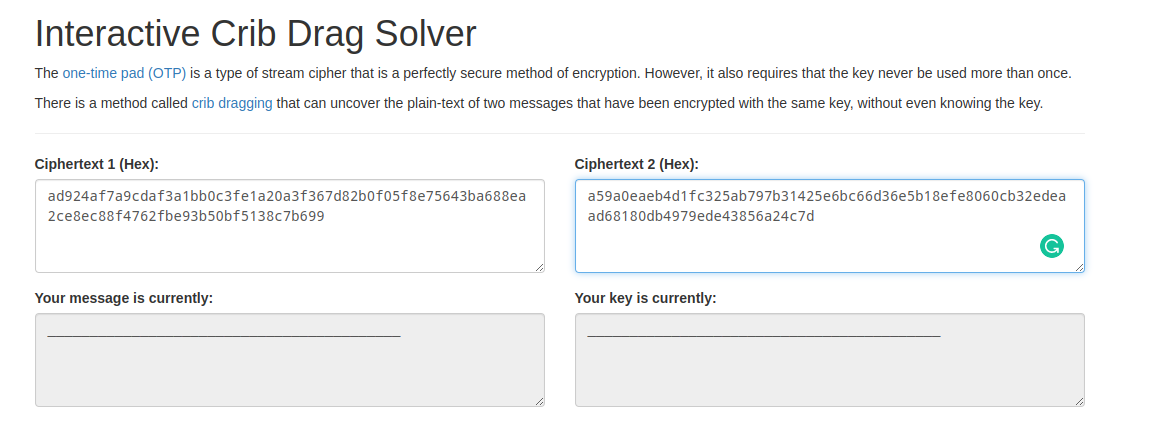
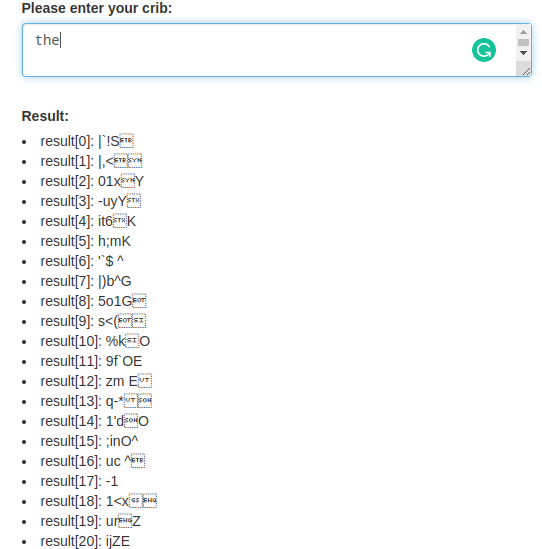
The one time pad (OTP) is a type of stream cipher that is a secure method of encryption. It’s simple to implement and is secure as long as the length of the key is greater than or equal to the length of the message. That’s its major downfall. However, it also requires that the key never be used more than once. This laboratory work shows what happens when you re-use a key to encrypt more than one message.  
We will use a method called crib dragging to uncover the plain-text of two messages that have been encrypted with the same key, without even knowing the key.  
  
Say we send messages A and B of the same length, both encrypted using same key, K. The stream cipher produces a string of bits C(K) the same length as the messages. The encrypted versions of the messages then are:  
  
E(A) = A xor C  
E(B) = B xor C  
where xor is performed bit by bit.  
Say an adversary has intercepted E(A) and E(B). He can easily compute:  
E(A) xor E(B)  
However, xor is commutative and has the property that X xor X = 0 (self-inverse) so:  
E(A) xor E(B) = (A xor C) xor (B xor C) = A xor B xor C xor C = A xor B  
E(A) xor E(B)  
However, xor is commutative and has the property that X xor X = 0 (self-inverse) so:  
  
E(A) xor E(B) = (A xor C) xor (B xor C) = A xor B xor C xor C = A xor B  
  
That means, if A and B were encrypted using the same key, we can decrypt A xor B

For resolving this task was used online Crib Drag Solver <https://lzutao.github.io/cribdrag/>

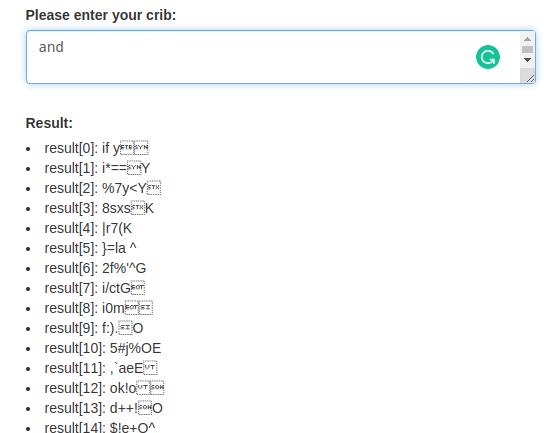


So, at first I am pasting two encrypted messages and then input cribs and analize.

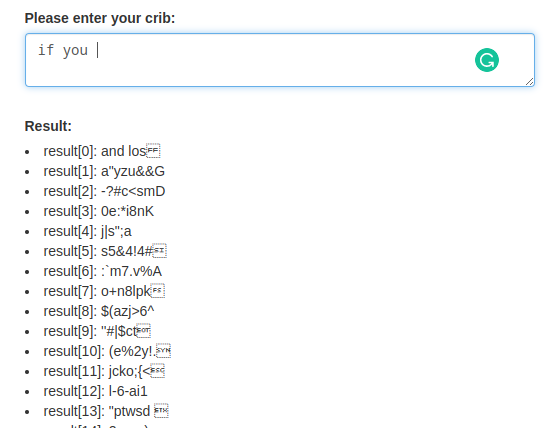
<https://en.wikipedia.org/wiki/Most_common_words_in_English> - list of the most used words in English.  
Let’s try first one - “the”. As we can see there are no words that are similar to English.



Let’s try “and” and we can see that there is “if y”



We can suppose that it can be if you, so lets try



We got “and los.” we can suppose futher and in such way step by step decrypting message.