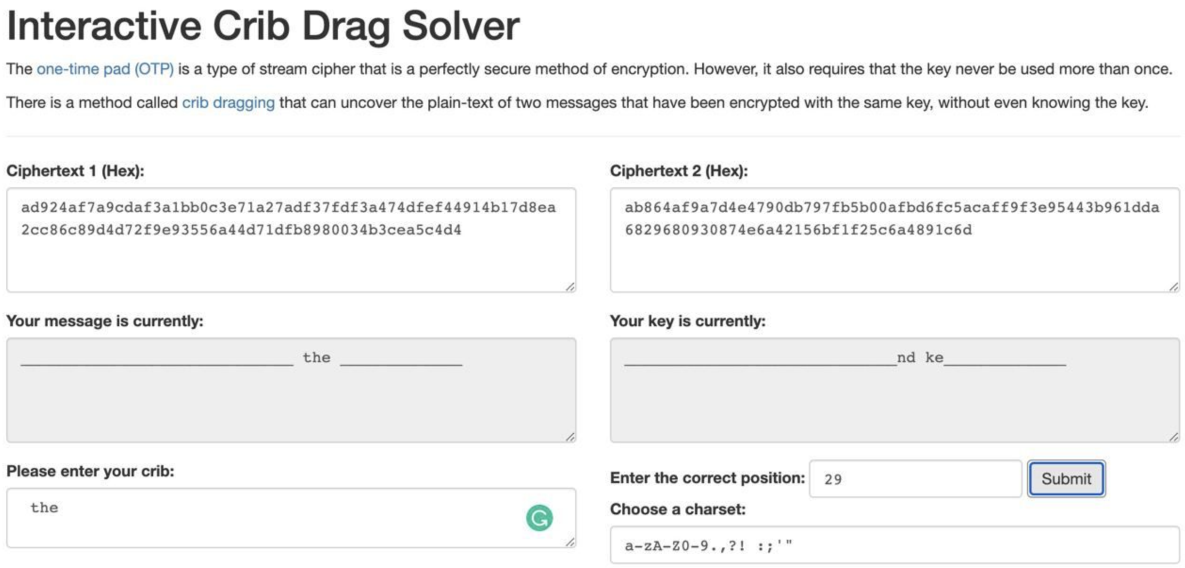
Lab 2 Report

For cracking this lab “crib dragging attack” was used with help of the online tool “Interactive Crib Drag Solver” (https://lzutao.github.io/cribdrag/). This attack is based on information that two ciphertexts were encrypted with the same key. All we need here - guess the words that possibly could be included in the first or second ciphertext. We can refer to a list of common used English words, to have more chances to succeed. Basically, the algorithm is the next:

1. Guess a word that might appear in one of the messages
2. Encode the word from step 1 to a hex string
3. XOR the two cipher-text messages
4. XOR the hex string from step 2 at each position of the XOR of the two cipher-texts (from step 3)
5. When the result from step 4 is readable text, we guess the English word and expand our crib search.
    a. If the result is not readable text, we try an XOR of the crib word at the next position.

Using online tool, we don’t need to care about XORing things, we just need to guess words.

Let’s see how it works. I started with the crib word “the” with spaces around and took the first two rows from the second part of the ciphertext.



Interactive Crib Drag Solver

The one-time pad (OTP) is a type of stream cipher that is a perfectly secure method of encryption. However, it also requires that the key never be used more than once.

There is a method called crib dragging that can uncover the plain-text of two messages that have been encrypted with the same key, without even knowing the key.

Ciphertext 1 (Hex):

```
ad924af7a9cdaf3a1bb0c3e71a27adf37fdf3a474dfef44914b17d8ea
2cc86c89d4d72f9e93556a44d71dfb8980034b3cea5c4d4
```

Ciphertext 2 (Hex):

```
ab864af9a7d4e4790db797fb5b00afbd6fc5acaff9f3e95443b961dda
6829680930874e6a42156bf1f25c6a4891c6d
```

Your message is currently:

```
_____________________________ the _____________
```

Your key is currently:

```
_____________________________nd ke_____________
```

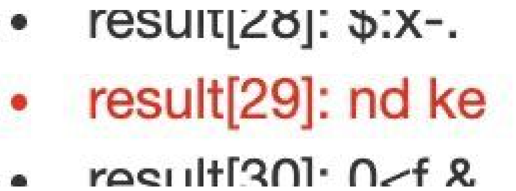
Please enter your crib:

```
 the 
```

Enter the correct position: 29 Submit

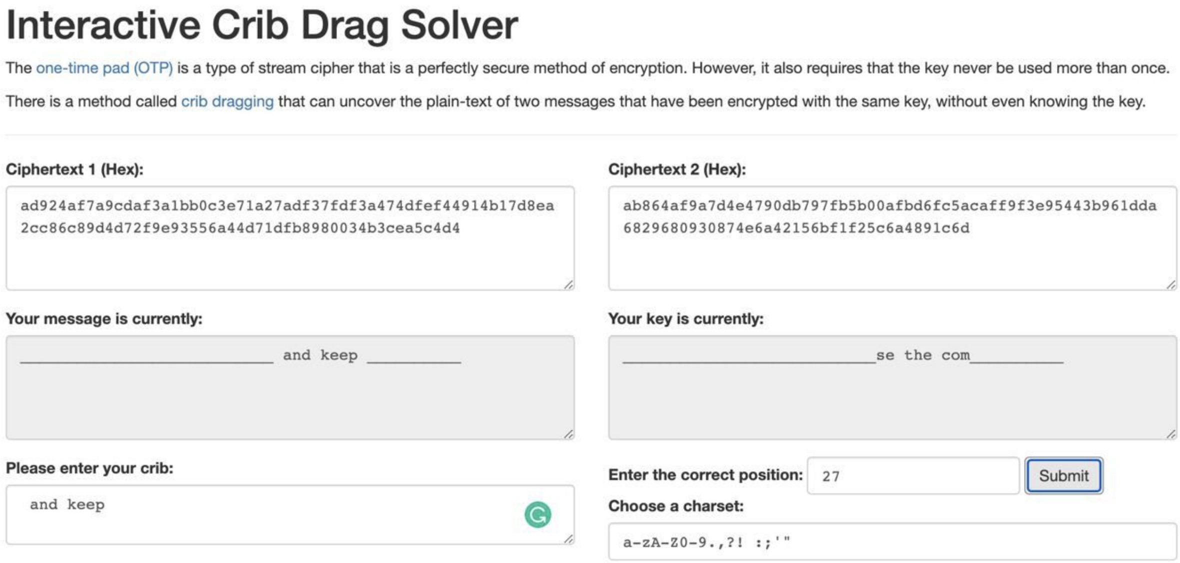
Choose a charset: a-zA-Z0-9.,?! :;'"

On the position 29 we can see something similar to real text, let's assume that it's a real part of the second ciphertext.



- result[28]: $:x-.
- result[29]: nd ke
- result[30]: 0<f &

Let's expand our search and assume that "nd ke" stands for " and keep " and try it as crib text.



Interactive Crib Drag Solver

The one-time pad (OTP) is a type of stream cipher that is a perfectly secure method of encryption. However, it also requires that the key never be used more than once.

There is a method called crib dragging that can uncover the plain-text of two messages that have been encrypted with the same key, without even knowing the key.

Ciphertext 1 (Hex):

```
ad924af7a9cdaf3a1bb0c3e71a27adf37fdf3a474dfef44914b17d8ea
2cc86c89d4d72f9e93556a44d71dfb8980034b3cea5c4d4
```

Ciphertext 2 (Hex):

```
ab864af9a7d4e4790db797fb5b00afbd6fc5acaff9f3e95443b961dda
6829680930874e6a42156bf1f25c6a4891c6d
```

Your message is currently:

```
___________________________ and keep __________
```

Your key is currently:

```
___________________________se the com__________
```

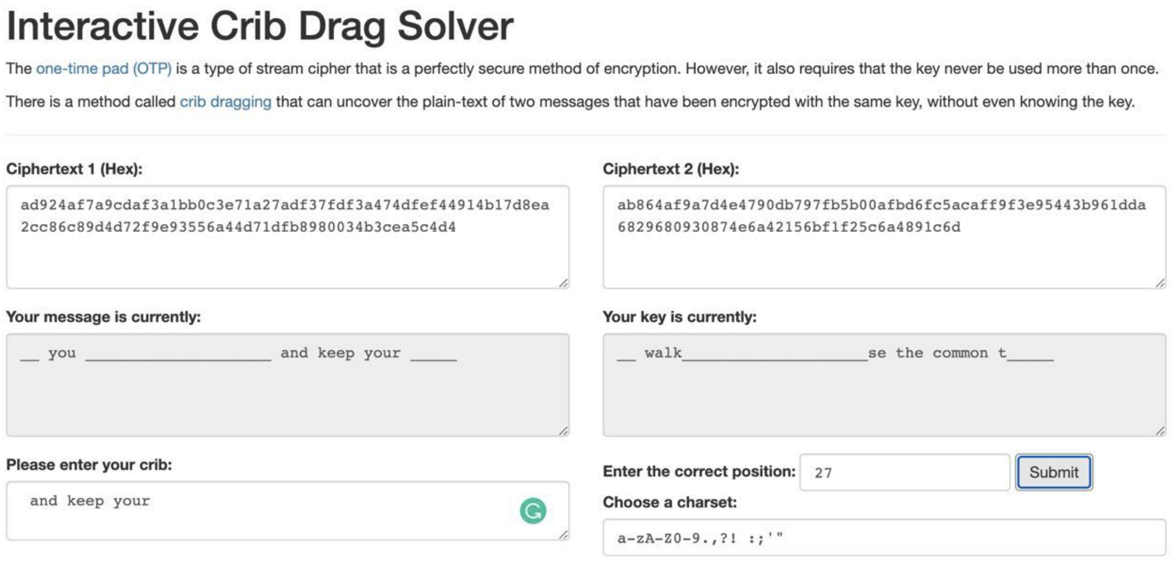
Please enter your crib:

```
and keep
```

Enter the correct position: 27 Submit

Choose a charset: a-zA-Z0-9.,?! :;'"

We've received some kind of readable text in another ciphertext. Let's continue with another common word "you". Fortunately, it turned out that "you" occurs twice in one of the ciphertexts. But in one case it's not just "you" but "yours".



Interactive Crib Drag Solver

The one-time pad (OTP) is a type of stream cipher that is a perfectly secure method of encryption. However, it also requires that the key never be used more than once.

There is a method called crib dragging that can uncover the plain-text of two messages that have been encrypted with the same key, without even knowing the key.

Ciphertext 1 (Hex):

```
ad924af7a9cdaf3a1bb0c3e71a27adf37fdf3a474dfef44914b17d8ea
2cc86c89d4d72f9e93556a44d71dfb8980034b3cea5c4d4
```

Ciphertext 2 (Hex):

```
ab864af9a7d4e4790db797fb5b00afbd6fc5acaff9f3e95443b961dda
6829680930874e6a42156bf1f25c6a4891c6d
```

Your message is currently:

```
__ you ____________________ and keep your _____
```

Your key is currently:

```
__ walk____________________se the common t_____
```

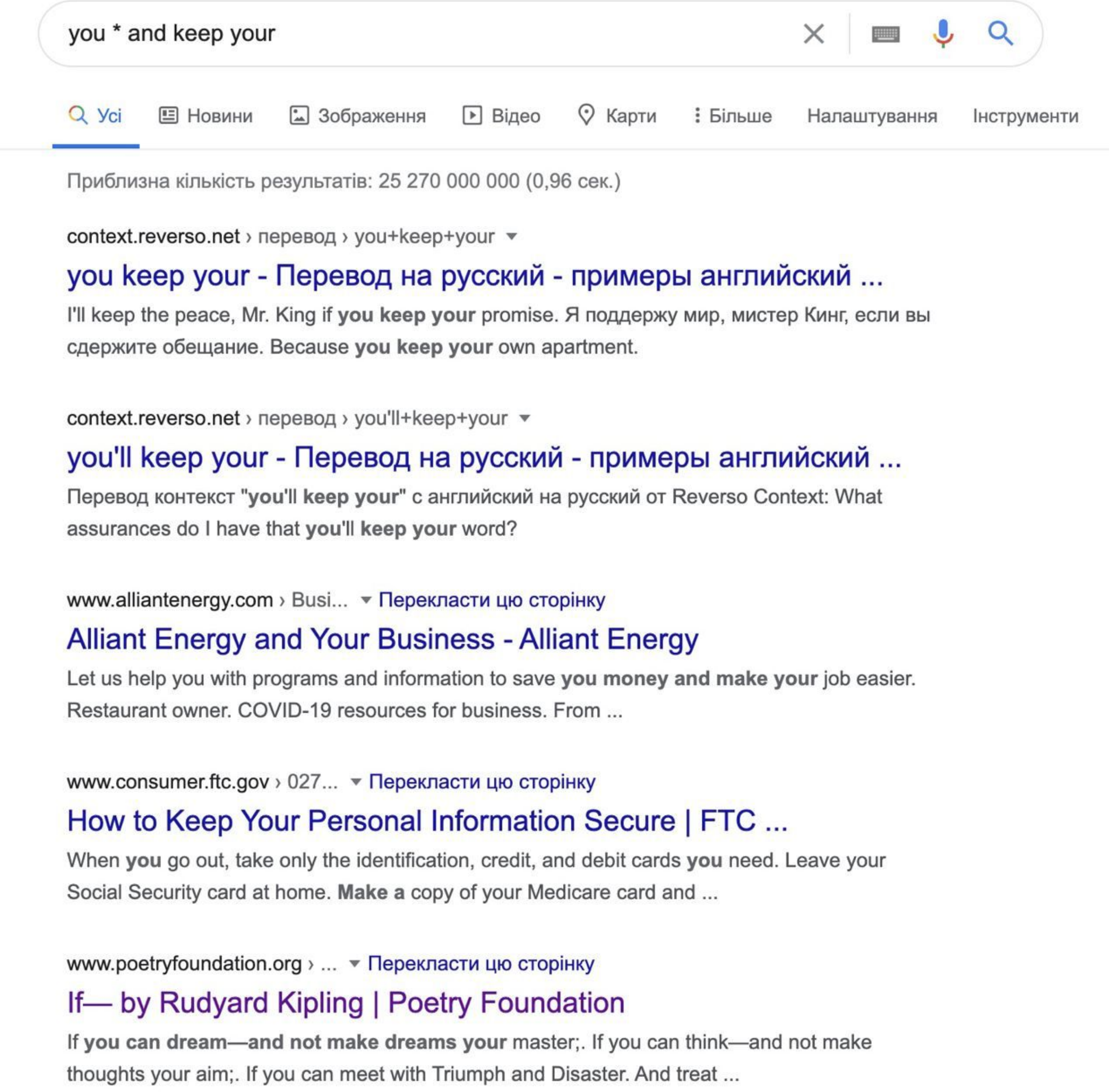
Please enter your crib:

```
and keep your
```

Enter the correct position: 27 Submit

Choose a charset: a-zA-Z0-9.,?! :;'"

Received result seems to be enough for trying google original text using search query “you * and keep your”.



Приблизна кількість результатів: 25 270 000 000 (0,96 сек.)

context.reverso.net › перевод › you+keep+your

you keep your - Перевод на русский - примеры английский ...

I'll keep the peace, Mr. King if **you keep your** promise. Я поддержу мир, мистер Кинг, если вы сдержите обещание. Because **you keep your** own apartment.

context.reverso.net › перевод › you'll+keep+your

you'll keep your - Перевод на русский - примеры английский ...

Перевод контекст "**you'll keep your**" с английский на русский от Reverso Context: What assurances do I have that **you'll keep your** word?

www.alliantenergy.com › Busi... Перекласти цю сторінку

Alliant Energy and Your Business - Alliant Energy

Let us help you with programs and information to save **you money and make your** job easier. Restaurant owner. COVID-19 resources for business. From ...

www.consumer.ftc.gov › 027... Перекласти цю сторінку

How to Keep Your Personal Information Secure | FTC ...

When **you** go out, take only the identification, credit, and debit cards **you** need. Leave your Social Security card at home. **Make a** copy of your Medicare card and ...

www.poetryfoundation.org › ... Перекласти цю сторінку

If— by Rudyard Kipling | Poetry Foundation

If **you can dream—and not make dreams your** master;. If you can think—and not make thoughts your aim;. If you can meet with Triumph and Disaster. And treat ...

As we can see there is a poem “If” written by Rudyard Kipling among the search results. If we check it we will assure that it was our original text.