# Many Time Secrets

AlexCTF 2017
Question Walkthrough

# What we are given:

https://github.com/ctfs/write-ups-2017/tree/master/alexctf-2017/cryptography/cr2-many-time-secrets-100

```
0529242a631234122d2b36697f13272c207f2021283a6b0c7908
2f28202a302029142c653f3c7f2a2636273e3f2d653e25217908
322921780c3a235b3c2c3f207f372e21733a3a2b37263b313012
2f6c363b2b312b1e64651b6537222e37377f2020242b6b2c2d5d
283f652c2b31661426292b653a292c372a2f20212a316b283c09
29232178373c270f682c216532263b2d3632353c2c3c2a293504
613c37373531285b3c2a72273a67212a277f373a243c20203d5d
243a202a633d205b3c2d3765342236653a2c7423202f3f652a18
2239373d6f740a1e3c651f207f2c212a247f3d2e65262430791c
263e203d63232f0f20653f207f332065262c3168313722367918
2f2f372133202f142665212637222220733e383f2426386b
```

This message + the fact that it was encrypted with  one time pad

# What is onetime pad??

“what is a one time pad”

http://users.telenet.be/d.rijmenants/en/onetimepad.htm

One-time pad (OTP), also called Vernam-cipher or the perfect cipher, is a crypto algorithm where plaintext is combined with a random key.

However, if only one of these rules is disregarded, the cipher is no longer unbreakable.

- **The key is at least as long as the message or data that must be encrypted.**
- **The key is truly random (not generated by a simple computer function or such)**
- Key and plaintext are calculated modulo 10 (digits), modulo 26 (letters) or modulo 2 (binary)
- **Each key is used only once, and both sender and receiver must destroy their key after use.**
- There should only be two copies of the key: one for the sender and one for the receiver (some exceptions exist for multiple receivers)

# How to crack a one-time pad?

Google

“how to crack a onetime pad”

https://crypto.stackexchange.com/questions/59/taking-advantage-of-one-time-pad-key-reuse

“The one time pad (OTP) is a type of stream cipher that is a perfectly secure method of encryption. It’s very simple to implement and is perfectly secure as long as the length of the key is greater than or equal to the length of the message.”

“Here, since the key is used more than one time, an attack called ‘crib dragging’ can be used to attack the cipher-text.”

# Crib dragging… How to do it?

https://github.com/SpiderLabs/cribdrag

“cribdrag is a script for performing crib dragging attacks against ciphertext encrypted using an XOR operation with a predictable key”

Google

“cribdrag tools”

**Download repo**

# Back to the message

Remove the newlines to reveal only the cipher text

```
cat msg | tr -d '\n'  > msg
```

```
cat msg
```

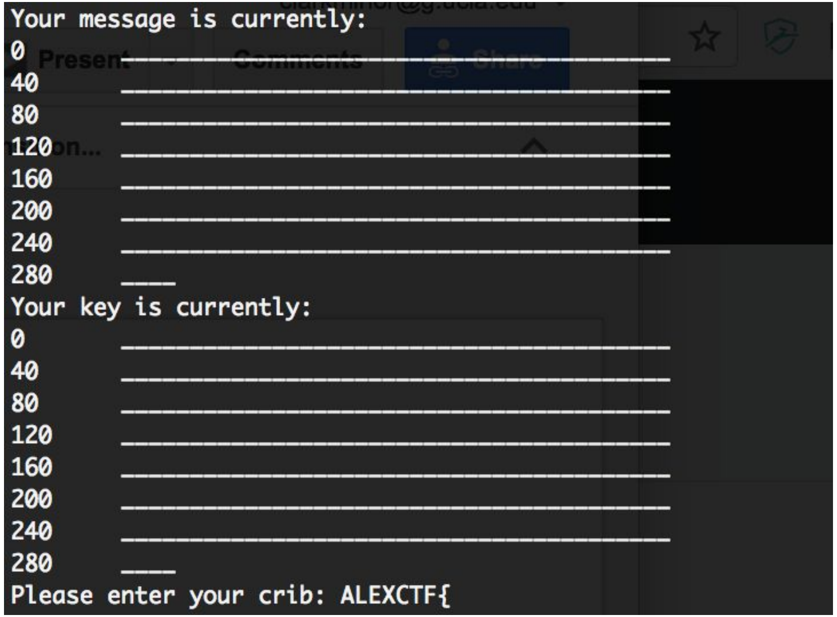
```
0529242a631234122d2b36697f13272c207f2021283a6b0c79082f28202a302029142c653f3c7f2a2636273e3f2d653e252179
08322921780c3a235b3c2c3f207f372e21733a3a2b37263b3130122f6c363b2b312b1e64651b6537222e37377f2020242b6b2
c2d5d283f652c2b31661426292b653a292c372a2f20212a316b283c0929232178373c270f682c216532263b2d3632353c2c3c
2a293504613c37373531285b3c2a72273a67212a277f373a243c20203d5d243a202a633d205b3c2d3765342236653a2c7423
202f3f652a182239373d6f740a1e3c651f207f2c212a247f3d2e65262430791c263e203d63232f0f20653f207f332065262c3168
3137223679182f2f372133202f14266521263722220733e383f2426386b
```

# Pass the message as the argument to the cribdrag tool

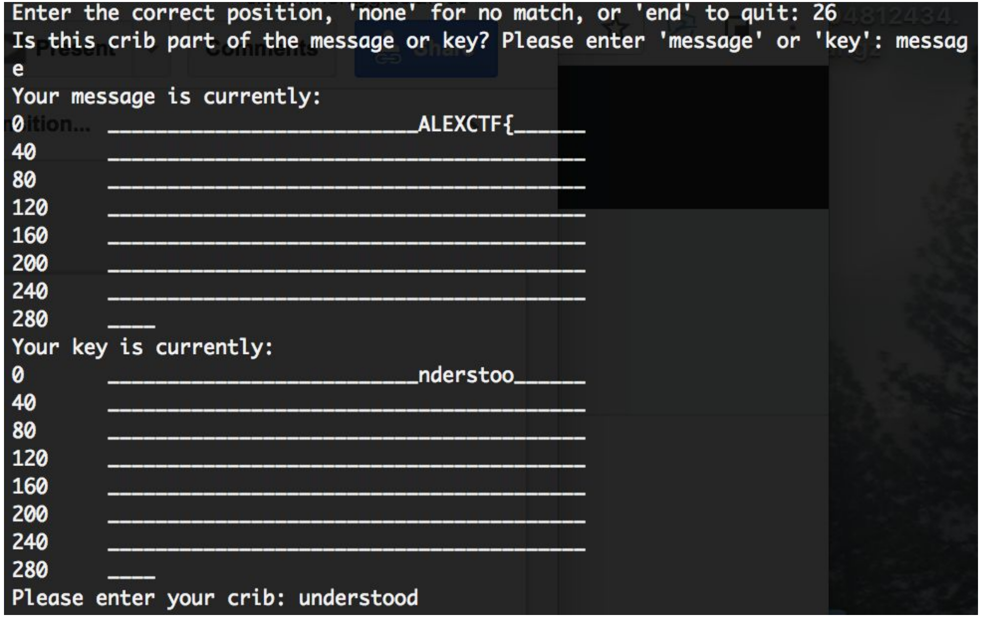
```
./cribdrag.py
0529242a631234122d2b36697f13272c207f2021283a6b0c79082f28202a302029142c653f3c7f2a2636273
e3f2d653e25217908322921780c3a235b3c2c3f207f372e21733a3a2b37263b3130122f6c363b2b312b1e6
4651b6537222e37377f2020242b6b2c2d5d283f652c2b31661426292b653a292c372a2f20212a316b283c0
929232178373c270f682c216532263b2d3632353c2c3c2a293504613c37373531285b3c2a72273a67212a
277f373a243c20203d5d243a202a633d205b3c2d3765342236653a2c7423202f3f652a182239373d6f740a
1e3c651f207f2c212a247f3d2e65262430791c263e203d63232f0f20653f207f332065262c31683137223679
182f2f372133202f142665212637222220733e383f2426386b
```

# Trial and Error!

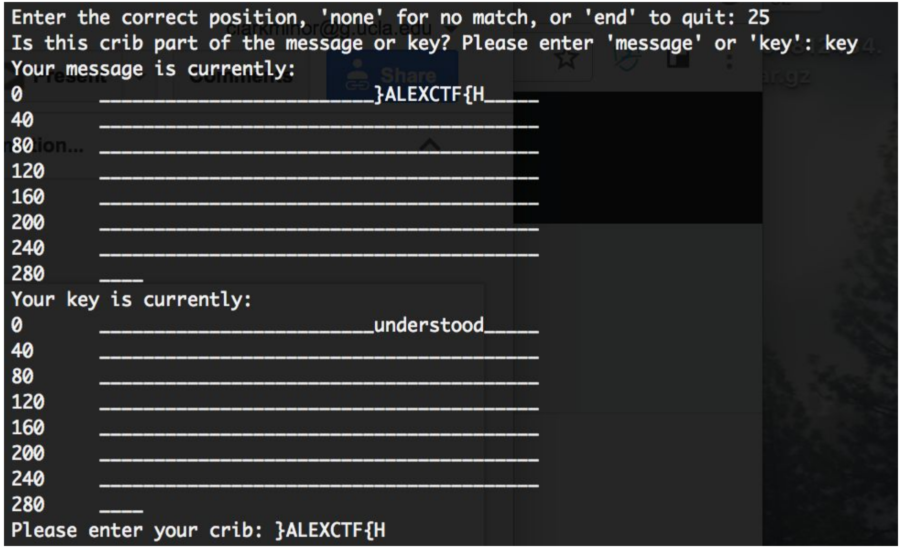
1) We know that the key will contain ALEXCTF{
2) We know that the key has been reused
3) We believe that the key is shorter than the length of the message, otherwise we would not be able to crack the message (we don’t have a second message to XOR with)



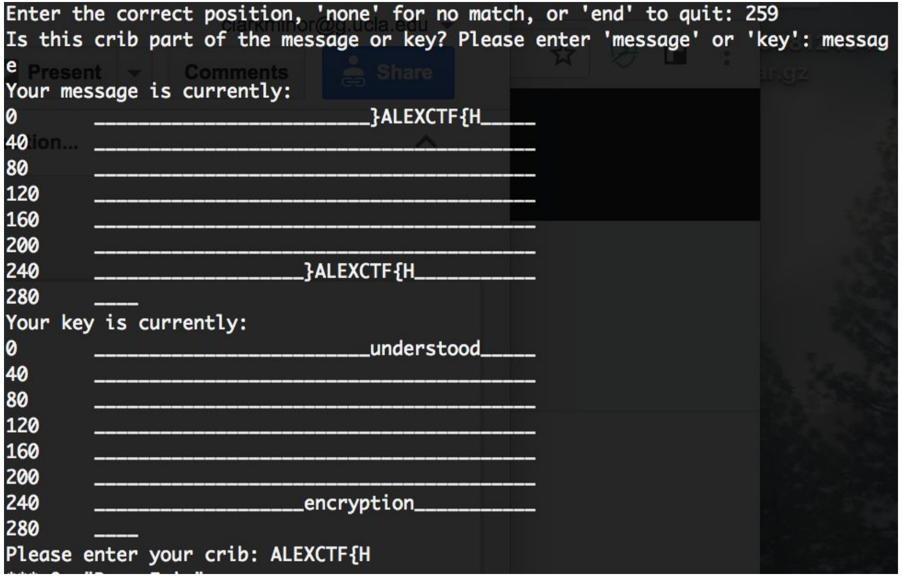
```
Your message is currently:
0       ________________________________________
40      ________________________________________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ________________________________________
280     ____
Your key is currently:
0       ________________________________________
40      ________________________________________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ________________________________________
280     ____
Please enter your crib: ALEXCTF{
```



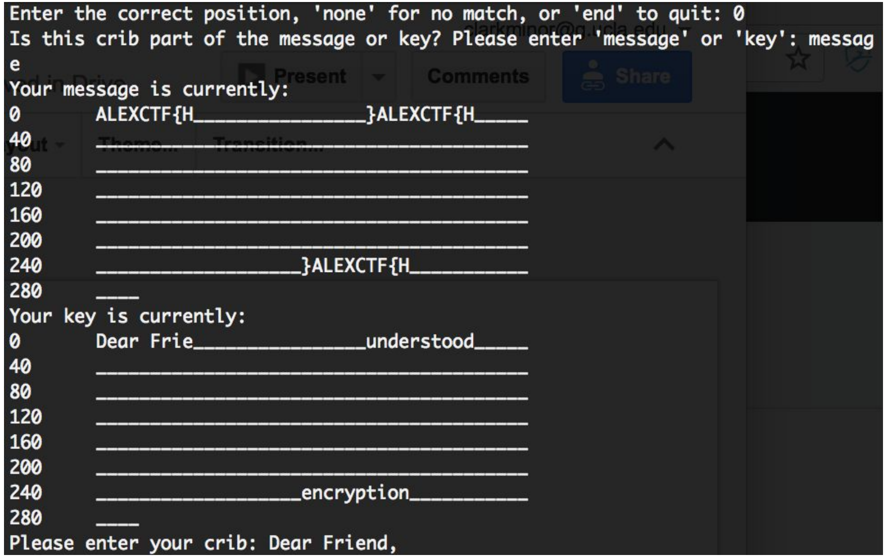
```
Enter the correct position, 'none' for no match, or 'end' to quit: 26
Is this crib part of the message or key? Please enter 'message' or 'key': messag
e
Your message is currently:
0       __________________________ALEXCTF{______
40      ________________________________________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ________________________________________
280     ____
Your key is currently:
0       __________________________nderstoo______
40      ________________________________________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ________________________________________
280     ____
Please enter your crib: understood
```



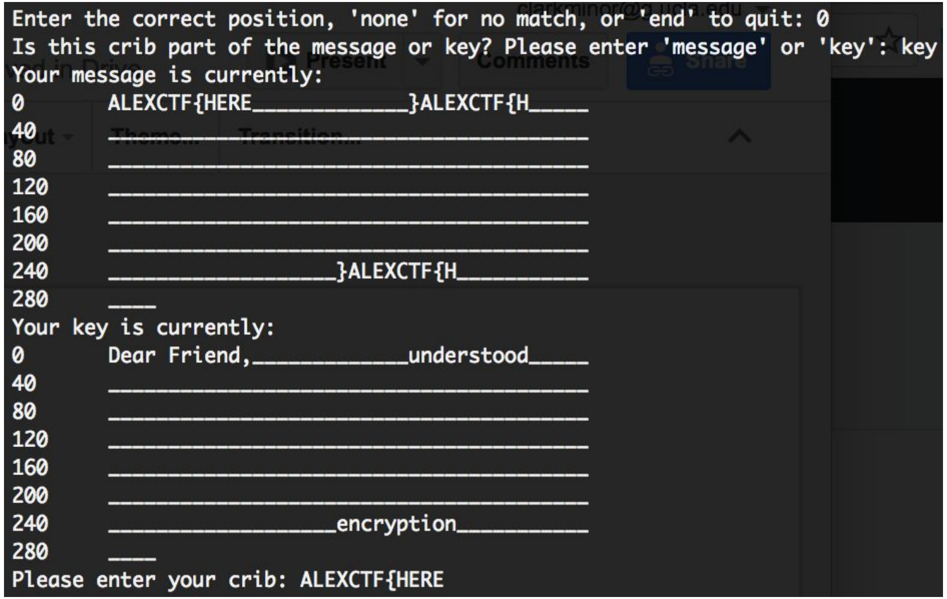
```
Enter the correct position, 'none' for no match, or 'end' to quit: 25
Is this crib part of the message or key? Please enter 'message' or 'key': key
Your message is currently:
0       _________________________}ALEXCTF{H_____
40      ________________________________________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ________________________________________
280     ____
Your key is currently:
0       _________________________understood_____
40      ________________________________________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ________________________________________
280     ____
Please enter your crib: }ALEXCTF{H
```



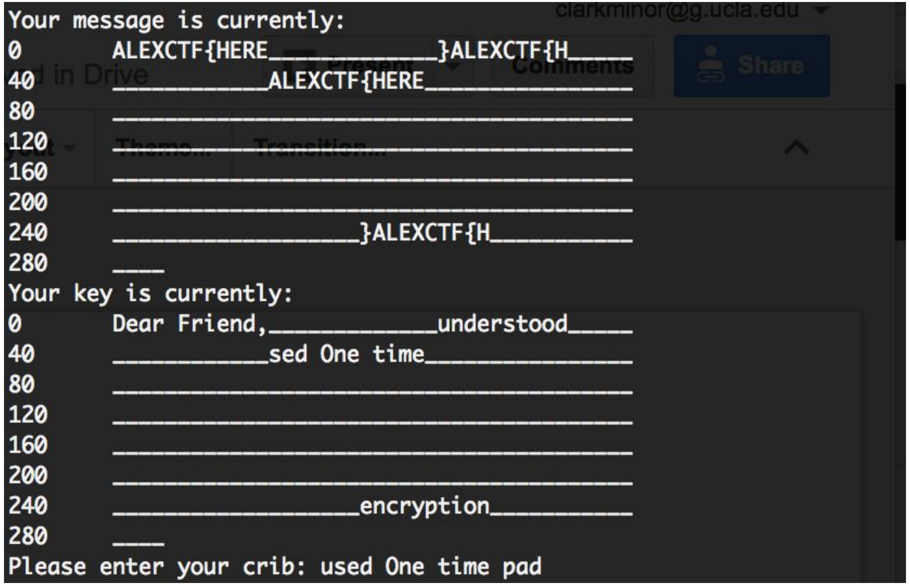
```
Enter the correct position, 'none' for no match, or 'end' to quit: 259
Is this crib part of the message or key? Please enter 'message' or 'key': messag
e
Your message is currently:
0       _________________________}ALEXCTF{H_____
40      ________________________________________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ___________________}ALEXCTF{H___________
280     ____
Your key is currently:
0       _________________________understood_____
40      ________________________________________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ___________________encryption___________
280     ____
Please enter your crib: ALEXCTF{H
```



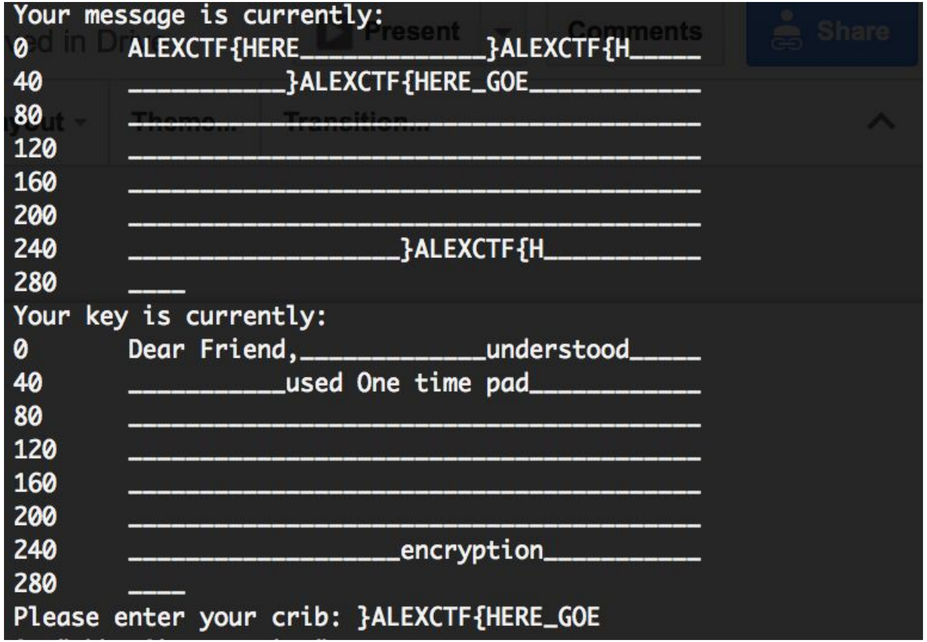
```
Enter the correct position, 'none' for no match, or 'end' to quit: 0
Is this crib part of the message or key? Please enter 'message' or 'key': messag
e
Your message is currently:
0       ALEXCTF{H________________}ALEXCTF{H_____
40      ________________________________________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ___________________}ALEXCTF{H___________
280     ____
Your key is currently:
0       Dear Frie________________understood_____
40      ________________________________________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ___________________encryption___________
280     ____
Please enter your crib: Dear Friend,
```



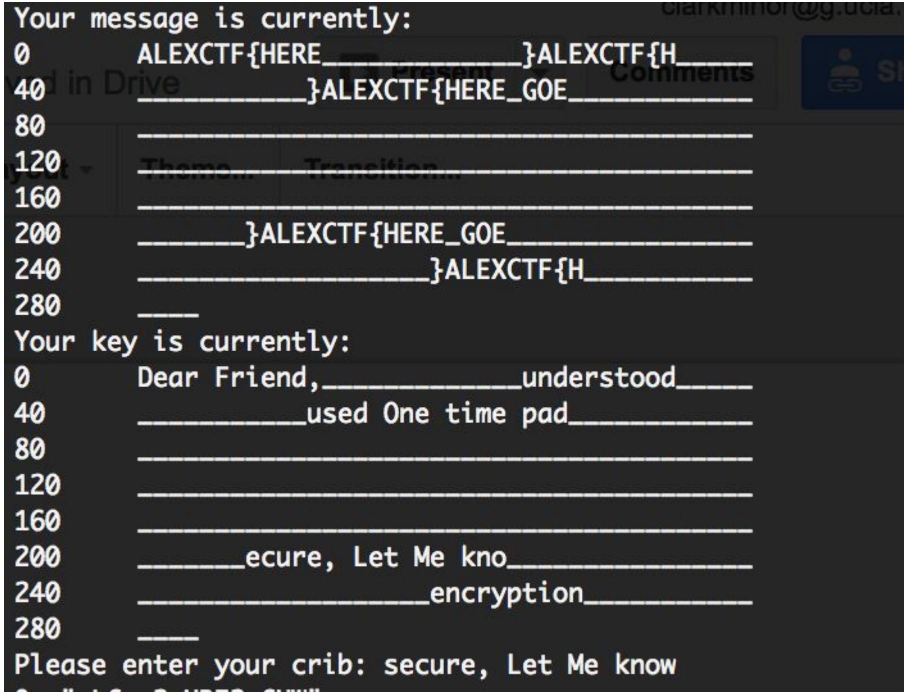
```
Enter the correct position, 'none' for no match, or 'end' to quit: 0
Is this crib part of the message or key? Please enter 'message' or 'key': key
Your message is currently:
0       ALEXCTF{HERE_____________}ALEXCTF{H_____
40      ________________________________________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ___________________}ALEXCTF{H___________
280     ____
Your key is currently:
0       Dear Friend,_____________understood_____
40      ________________________________________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ___________________encryption___________
280     ____
Please enter your crib: ALEXCTF{HERE
```



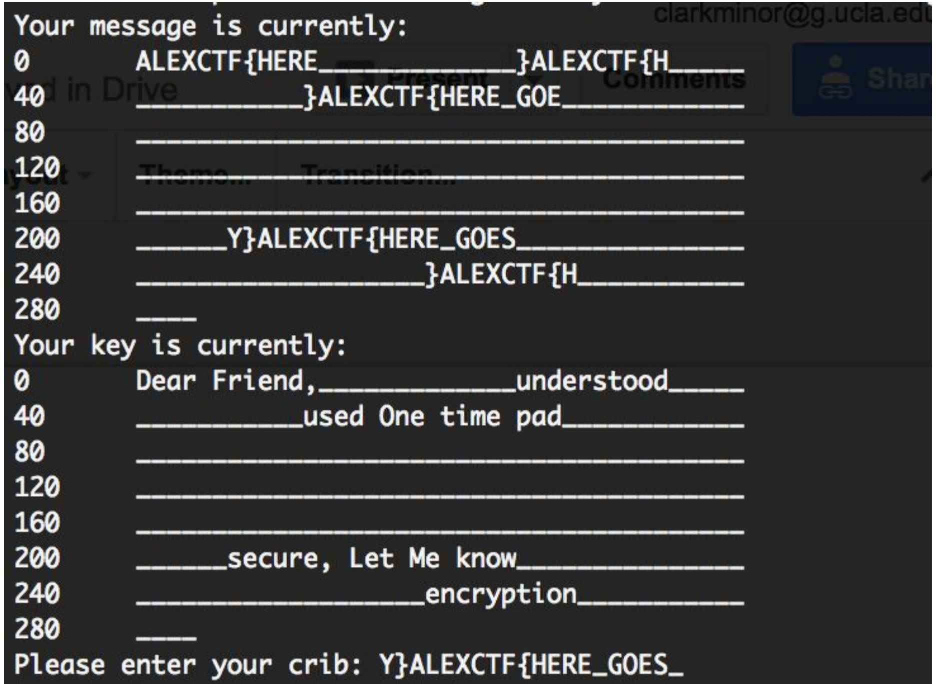
```
Your message is currently:
0       ALEXCTF{HERE_____________}ALEXCTF{H_____
40      ____________ALEXCTF{HERE________________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ___________________}ALEXCTF{H___________
280     ____
Your key is currently:
0       Dear Friend,_____________understood_____
40      ____________sed One time________________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ___________________encryption___________
280     ____
Please enter your crib: used One time pad
```



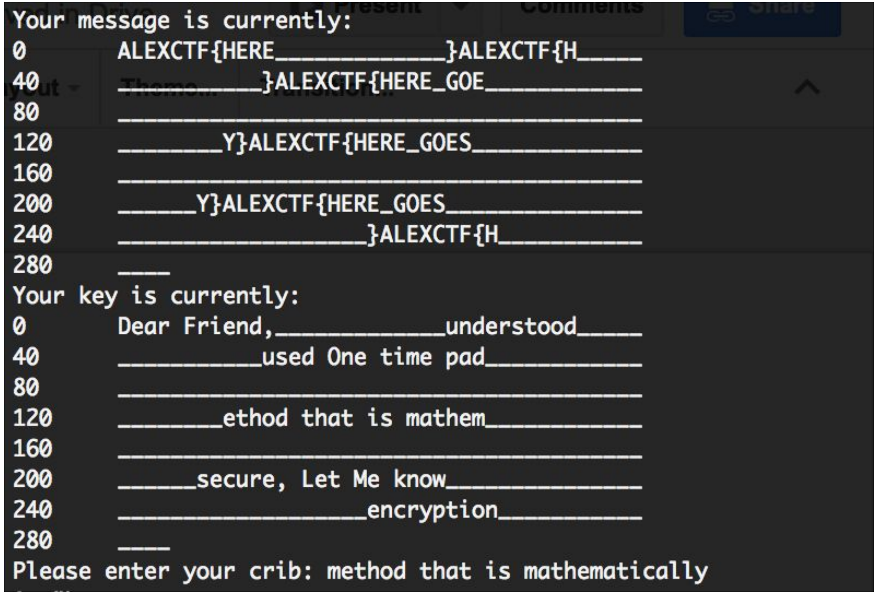
```
Your message is currently:
0       ALEXCTF{HERE_____________}ALEXCTF{H_____
40      ___________}ALEXCTF{HERE_GOE____________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ___________________}ALEXCTF{H___________
280     ____
Your key is currently:
0       Dear Friend,_____________understood_____
40      ___________used One time pad____________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ________________________________________
240     ___________________encryption___________
280     ____
Please enter your crib: }ALEXCTF{HERE_GOE
```



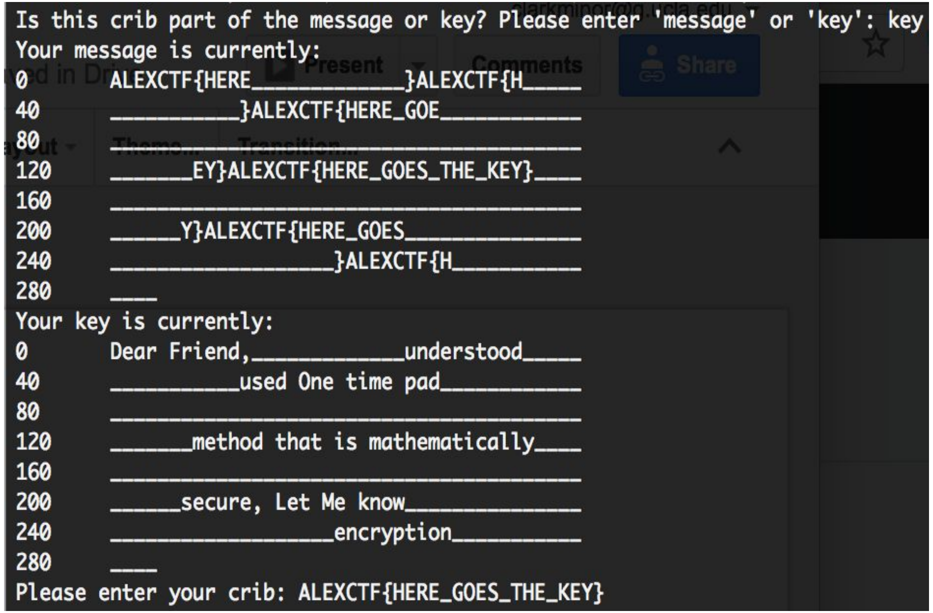
```
Your message is currently:
0       ALEXCTF{HERE_____________}ALEXCTF{H_____
40      ___________}ALEXCTF{HERE_GOE____________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     _______}ALEXCTF{HERE_GOE________________
240     ___________________}ALEXCTF{H___________
280     ____
Your key is currently:
0       Dear Friend,_____________understood_____
40      ___________used One time pad____________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     _______ecure, Let Me kno________________
240     ___________________encryption___________
280     ____
Please enter your crib: secure, Let Me know
```



```
Your message is currently:
0       ALEXCTF{HERE_____________}ALEXCTF{H_____
40      ___________}ALEXCTF{HERE_GOE____________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ______Y}ALEXCTF{HERE_GOES_______________
240     ___________________}ALEXCTF{H___________
280     ____
Your key is currently:
0       Dear Friend,_____________understood_____
40      ___________used One time pad____________
80      ________________________________________
120     ________________________________________
160     ________________________________________
200     ______secure, Let Me know_______________
240     ___________________encryption___________
280     ____
Please enter your crib: Y}ALEXCTF{HERE_GOES_
```



```
Your message is currently:
0       ALEXCTF{HERE_____________}ALEXCTF{H_____
40      ___________}ALEXCTF{HERE_GOE____________
80      ________________________________________
120     ________Y}ALEXCTF{HERE_GOES_____________
160     ________________________________________
200     ______Y}ALEXCTF{HERE_GOES_______________
240     ___________________}ALEXCTF{H___________
280     ____
Your key is currently:
0       Dear Friend,_____________understood_____
40      ___________used One time pad____________
80      ________________________________________
120     ________ethod that is mathem____________
160     ________________________________________
200     ______secure, Let Me know_______________
240     ___________________encryption___________
280     ____
Please enter your crib: method that is mathematically
```



```
Is this crib part of the message or key? Please enter 'message' or 'key': key
Your message is currently:
0       ALEXCTF{HERE_____________}ALEXCTF{H_____
40      ___________}ALEXCTF{HERE_GOE____________
80      ________________________________________
120     _______EY}ALEXCTF{HERE_GOES_THE_KEY}____
160     ________________________________________
200     ______Y}ALEXCTF{HERE_GOES_______________
240     ___________________}ALEXCTF{H___________
280     ____
Your key is currently:
0       Dear Friend,_____________understood_____
40      ___________used One time pad____________
80      ________________________________________
120     _______method that is mathematically____
160     ________________________________________
200     ______secure, Let Me know_______________
240     ___________________encryption___________
280     ____
Please enter your crib: ALEXCTF{HERE_GOES_THE_KEY}
```

# There it is!!!

ALEXCTF{HERE_GOES_THE_KEY}

Great, so we found the key. And all without any previous knowledge of what a one time pad was!!