Encrypting a 3 letter word with a One Time Pad:

- do the first two	questions	with your	partner
--------------------	-----------	-----------	---------

- 1) Agree on a secret key with your partner (fill this in for k)
- 2) If encryption is done via XOR, how should description be done? (fill in the blank)

- do the next two questions by yourself

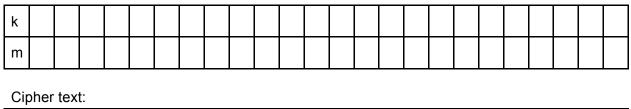
- 3) Wait for the cipher text from your partner.
- 4) Decode the cipher text to recover the original message.

De	Decryption: (what is the inverse of XOR?)																			
k																				
С																				
Message:																				
m																				

What is the message (in ascii)?

- next, you will repeat the exercise but you will encode a message for your partner
 - 5) Agree on a different secret key with your partner (fill this in for k)
 - 6) Choose a **secret** message that is 3 letters long and fill in the binary below.

Encryption: XOR



7) Tell your partner the resulting cipher text.

One Time Pad security + usage

- What happens if we use the same One Time Pad twice? What information would an eavesdropper have access to?
 What information about the messages would the eavesdropper be able to recover? (What is c1 XOR c2 equivalent to? Where c1 is the first cipher text and c2 is the second cipher text)
- 3) If I have a message of n bits, how many bits must my One Time Pad be?