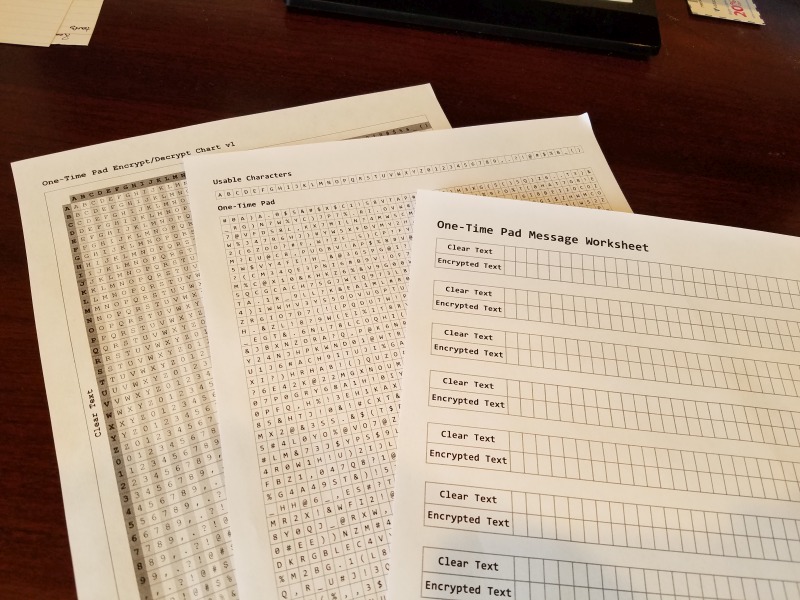
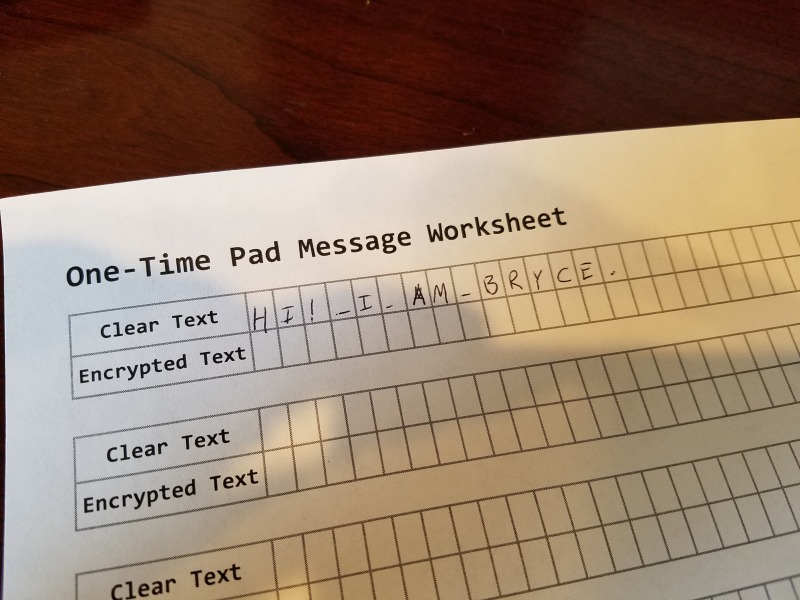
**Using the One-Time Pad**

**Encrypting a Message**

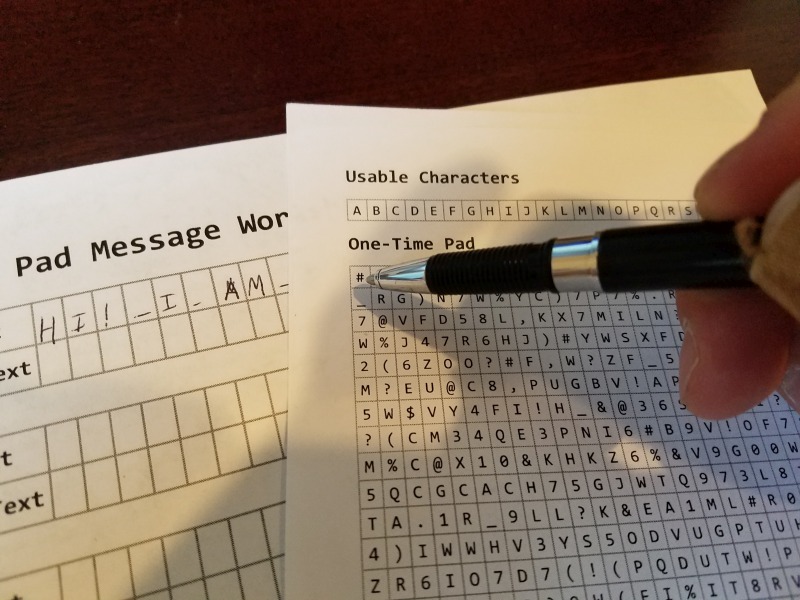
First, get the things I mentioned above.



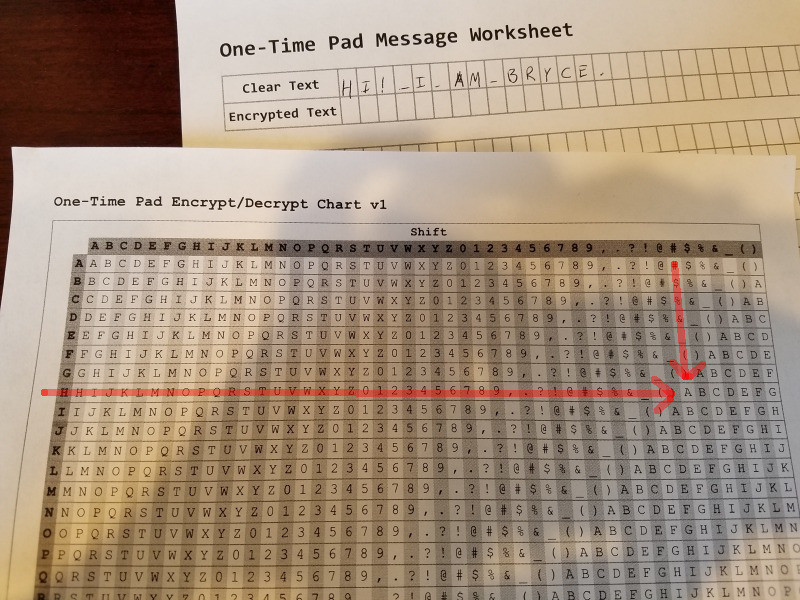
Once you’ve printed two copies of your one-time pad and given one to your messaging partner, it’s time to encrypt your first message. Write the message you want to encrypt in some boxes on a message worksheet. I’ll encrypt the message **HI! I AM BRYCE.** And I will use underscores for the spaces. Some people just omit the spaces altogether.



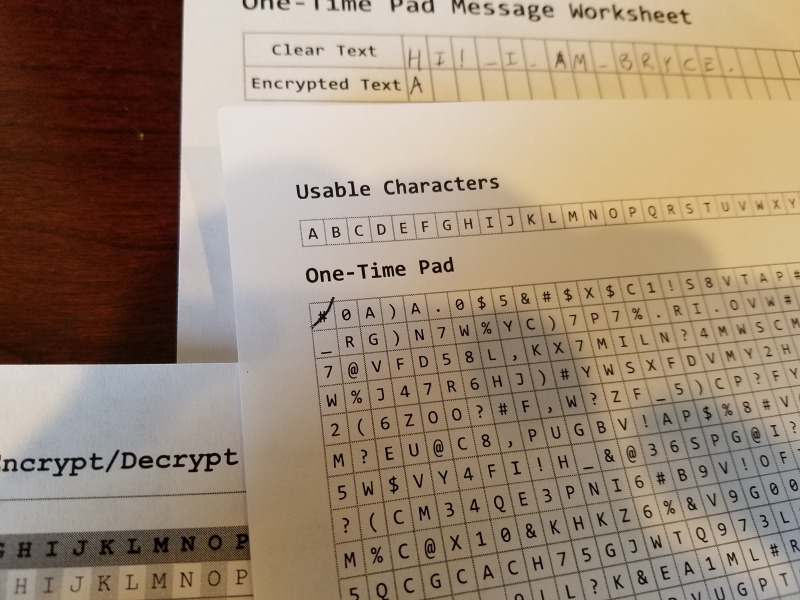
Look at the first box on your one-time pad. The character in that box will be the “shift” for your first character.



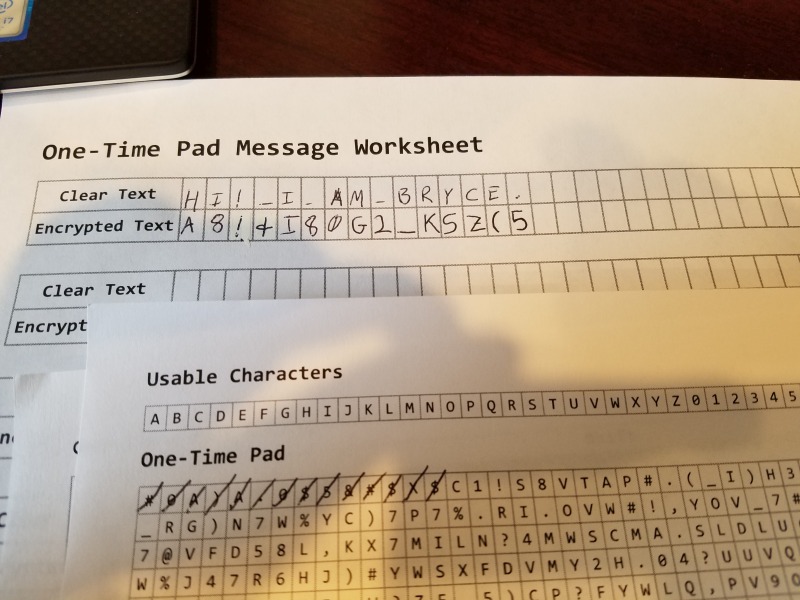
On your Encrypt/Decrypt chart, scan down the leftmost column to find the row with your “Clear Text” character, in my case an “H”. Then move to the right until you are in the column of the “Shift”, in this case “#”. the box where that row/column intersect is your encrypted text. In this case, it is an “A”.



Now cross off that first square of your one-time pad. You will never use that square again.



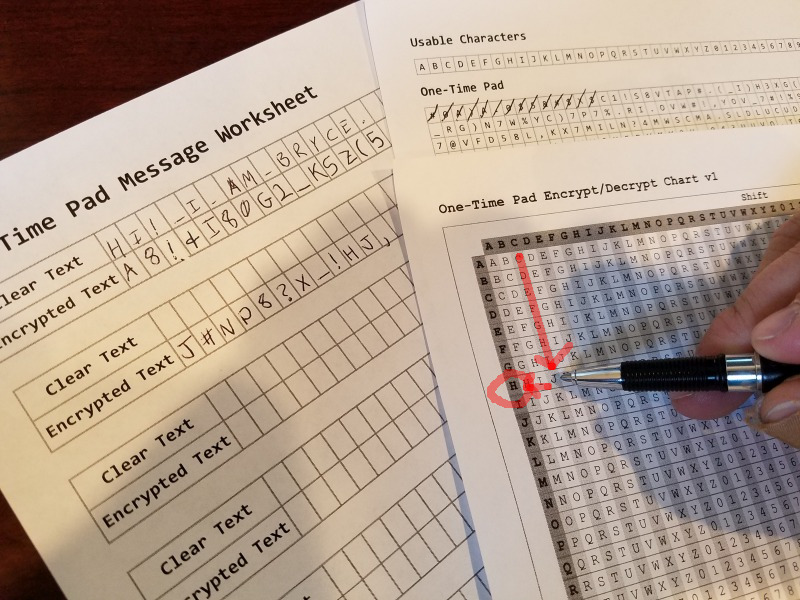
Continue, using one square on your one-time pad for each character in your message. Remember to cross out each square as you use it. Here’s my message, encrypted.



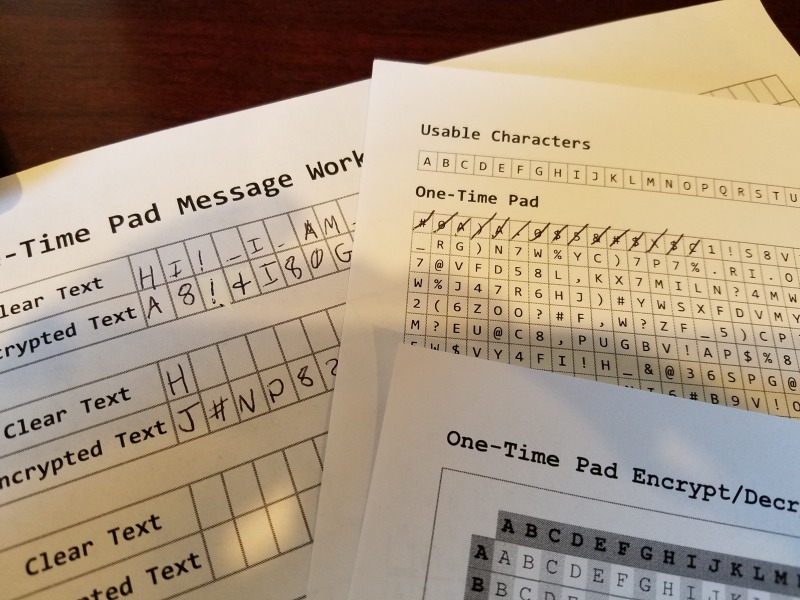
Now you are done! Write the encrypted message on another piece of paper, or send it in an email or a tweet. It doesn’t matter who else sees it, because it is encrypted!

**Decrypting a Message**

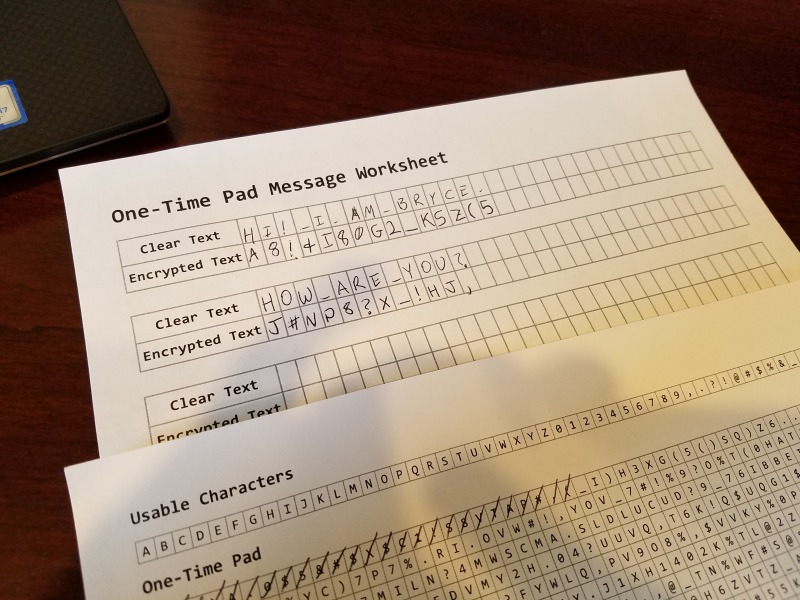
Now your friend has received and read your message, and sent you a message, **J#NP8?X\_!HJ,**  . Continue using the remaining boxes on the same one-time pad. For ease, you can write the encrypted message on a worksheet. Take note of the next open box on your one-time pad, this is the “shift”. Then follow the column down until you see the encrypted text. Go left to discover the clear text. In my example, I scan the first row until I see the column that has the “shift”, in my case the “C”. Then I look down that column until I see the encrypted text, in my case a “J”. I follow the row left to discover what the clear text character is. In my case it’s an “H.”



Write the clear text character above the encrypted text character on your worksheet, cross off the used shift on the one-time pad.



Now I continue in the same pattern until all characters have been decrypted.



**Keeping it Secure**

If you do two things, you’ll keep your notes ultra secure.

1. One-Time pad means use it ***one time***. Once you use up the pad, generate another and use it.
2. Both parties must keep their copies of the pad safe.

**Weaknesses**

1. I’m using javascript’s built-in random number generator. Mathematically speaking, it is only pseudo-random, not “truly” random. Maybe someday I’ll make a version that uses random.org’s api. Random.org uses atmospheric data which is much more “actually” random. For a regular person, though, I think you’ll be fine.