Mandatory crypto assignment 1

There is several reasons why using the same key for one-time pad is a bad idea, first off it would not be true one-time pad if you use the same key, the primary idea behind one-time pad is to use a truly randomized key for each time you encrypt with it. The second is that the key used for one-time pad is supposed to be at least the same length as the data you need encrypted meaning if you only have a 100 bit key, you can only encrypt 100 bit data.

The idea of a key with the same length as the data you encrypt is that each symbol encrypted will have its own key, and a 10 letter text is encrypted it could be decrypted to many possible text, so if one was to try and brute force the encryption they could get a text that make sense, but would not know whether it is the correct text. If some one gets their hands on 2 texts encrypted with the same key, one could use the second text as a checksum, so when you get a text that makes sense you can check up on the other text to see if that too makes sense.

Magnus Holgersen