Richard Hayes Crowley

06/17/2021

CSC\_242\_Lab\_04 Q&A

**(1)** What is meant by a transposition cipher?

**A transposition cipher is a position-based or index-based cipher that references the position or index of an item in a plaintext list with the item in an encrypted list. It could be a Dictionary<int:string> type, or a nested Tuple<(int,string)>, etc., or some other object that maps the index or position of the plaintext with the index or position of the encrypted text.**

**(2)** What if we took the plaintext and split it into two separate lists. Then, we can reverse the two lists and concatenate the resulting lists. Would this be a good way to disguise your plaintext message? Explain your answer.   
  
**I don’t think so, since even when reversed, the two separate lists would still have recognizable patterns. E.g.,**

**strMsg = "The Courier is En Route with the Documents"**

**strMsg1 = [i for i in strMsg[0:len(strMsg) // 2]]**

**strMsg1.reverse()**

**strMsg2 = [i for i in strMsg[len(strMsg) // 2:]]**

**strMsg2.reverse()**

**print("".join(strMsg1), "".join(strMsg2))**

**Returns this string, which has recognizable patterns in it:**

**uoR nE si reiruoC ehT stnemucoD eht htiw et**

**(3)** What if we did not randomly scramble the plaintext characters but instead simply perform what is known as a Caesar shift? Would this be a more secure method of encryption?  
  
**No, as you can programmatically discover the “shift” number used in the Caesar shift, whether it is shifted by 3 or 7 etc., and then the entire cipher is broken. This would involve a nested loop within an encrypted list and the alphabet, and testing the word’s coherence against a dictionary. If you find one meaningful word, then the distance between the encrypted letters and the plaintext letters would be your shift number. This can then be used to decipher the rest of the text… however, a Caesar shift could be a good red herring, giving the code cracker the illusion of finding the plaintext.**

**(4)** How about using the list **sort()** method for concealing a message? Would that be a good idea?

**Sure, if you pass in a function to the optional ‘key’ parameter that uses nuanced logic to sort characters. Sorting by ascending or descending based on a letters position in the alphabet is not secure at all… however, if you had passed in a lambda function that sorted against a special cipher, then you could be in business.**

**(5)** What have you learned from performing and coding for this lab assignment?

**Got some great practice with list manipulation and methods, as well as some practice with cryptography.**