

**Exercise Set 2.****Due in Class on Wednesday, February 28****Write as if this were part of your resume for a high-paying job you really want!**

1. Recall the definition of a (good) *riffle shuffle* given in the text, and consider a perfect *overhand shuffle* that divides the deck into two equal parts and interchanges the two parts. Consider a deck of 12 cards. Suppose one alternates a riffle shuffle with a perfect overhand shuffle.

(a) What is the disjoint cycle decomposition of a riffle shuffle followed by an overhand shuffle?

(b) How many repeats are necessary until the cards return to their original positions?

2. Try a Kasiski attack on the following ciphertext:

CNPWVBAGYWOFGWCIYBQZDELTAAABADAAGHLDLPHDDNZYCKFPPUUPPJC  
 HUPFCFPBQXAACUFMPPNLOYPALDNVAZDDMWZJPMXFJYDKCYPVNFJLY  
 KLTPLGYFDPALFRIKKXUMYYJPMTBCNPWVBAGYWOFGWCIYGNVMRDGDKF  
 PKOZARKKKAJGDDNBQFQBVRLIQNQDMQGDFYPHLDQGHQMATGIJPMATJ  
 EUKBUUDRKKIVACQACKNKIGIEFQKRKZU

What are your conclusions about the key length?

3. The cipher text

OCXJIW JCBR JC XDQCO KFBKGDFQ GK REC XJICV ZBDLPB WLS  
 DM EMJC CPLK TMOI XLA BLLQ RBJI YKWYMAW

was obtained using a Vigenère cipher with a key of length 2. Decrypt it!

4. Determine the expected distance between two **e**'s in a random character stream where **e**'s occur 11% of the time (and thus the other characters taken as a whole occur 89% of the time).

PTO

5. Consider the game of *craps* played as follows: The shooter rolls two dice. He wins outright if the first roll is a 7 or 11, loses if it is 2, 3, or 12. Otherwise, he must repeatedly roll until his score is repeated (he wins!) or a 7 appears (he loses!). Compute the expected number of rolls until the game terminates.