ECE6280
Project 1
Due Wednesday September 11, 2019

Aug 26, 2019

1 Problem 1 (10 points)

Break the following Vigenère Cipher, which encrypts an English text.:

```
yysjxbysjxnkwkpjucfhyeswwyysotqc
vwbxrzdinessgizoetugzwhwtvski
dmsiucslkjvgobqcbwojiuwmftfglx
rbvxfkhzxhfbwlzerwkmzghbsvgamjczzbr
ysggqpgsrxxcgwkvbuxxdocxlfcvgjzuzutig
kiwzbybxkvwfnjqzbjwwffjrbvbbfbvxw
ztavtlzvizkofhyzcfbsywkajrr
oaduclajpasdjxcgwsvwyagffkbxeham
bysjxyysjxfisuhbjpmmmvfwmmvfwtwvbgvtng
txkffwbglwdmfnodenuokdyfyfhb
nvsmnnokpfczaglzbgkbrzdbsxcmm
ferlhbycebbrgdbpvhgznmsgykvbkx
xfawmmzbymmvfwbxkvsmifskgyccnxfnode
yyolpfehkbyucogntcmeijoqxqmskmtywe
uzkwllsfhweavgwqfthdrferawwrhzxw
ysktnuwlytivafxvzxbxvszbrkvwkj
sfaglzbytxkcfxliokijutakrcmtryyslhu
zbwthyvsgicwcxfecdwxkcfxxrjszjrfexi
ysehavgagirfcgjjgslnkgwxrjhgfj
eclhkncgwxfbdrferlajjvswjftlkjvg
zxbzzdgtkugujywfwmzgxtyysjlxrmagl
rbvajcwcxxyonbsxhzhzxvlhkzhkhbvzd
ajjoqlfxoaglfcvyjeqwlrrywztfrfxnxvthwj
```

The first thing is to find the length of the key. Do either the index of coincidence method or the Kasiski test work? If so, which or both? Have fun! Use the following table of probabilities of English letters. The spaces

between words have been deleted.

letter	probability
A	0.082
B	0.015
C	0.028
D	0.043
E	0.127
F	0.022
G	0.020
H	0.061
I	0.070
J	0.002
K	0.008
L	0.040
M	0.024
N	0.067
O	0.075
P	0.019
Q	0.001
R	0.060
S	0.063
T	0.091
U	0.028
V	0.010
W	0.023
X	0.001
Y	0.020
Z	0.001

2 Problem 3 (5 points)

The following two messages have been encrypted with a one-time pad. However, the person responsible to do the encryption forgot to change the one-time pad key and both messages are encrypted with the same key. Hint: The first message starts with the word "four" and the second starts with the word "now". Decrypt these two messages. Don't waste too much time on this.
'Bccxfcuebxmymiaaydkjazaytgujkbgwrbsgrgylzxknuouxndzlb
xpfesrnaerxnoagbeseppdnntymrvwvnbwgjylnlvhipcsyyugqugzm
yksrblwjrowiswbdonwodvcsntkgqyrtbho'
and
'jcecraxrbkfvaiieyfmanhtunnidbbeirctnnyamwxmduoujtxswrj
ogckrhalksxffukkrtrjlpmlqlgbmoiiupjeocifotugwsxleg'