

## MATH 445, HOMEWORK 2

1. The following text has been enciphered with a Caesar shift.

KTMZSIJRCZMZMVDGAGVKIVBZWWN

What are the two most probable keys? Is it evident which one is correct?

2. Decrypt the following Vigenère-enciphered text:

```
yaeosizdscqniqmsyuzebqdkx
yjhdiwmutmdtefsmqlrkliku
aeevydzdzqerfoiugilneijb
espijjursmfkulrnannxyrgus
wqnlddtfeelhytftcbavvhcg
d
```

In your solution, give both the keyword and the plaintext. A text file containing the ciphertext is linked on the course website so that you can copy-paste from it.

3. An urn contains 9 ping-pong balls, each of which is either white or orange. You don't know how many of each color there are, and you have no initial reason to believe that any split is likelier than any other split; that is, you believe that each of the 10 possibilities each have probability  $1/10$ .

You now draw four balls from the urn *with replacement*: that is, you draw a ball randomly from the urn, observe its color, and put it back in the urn, and you do this a total of four times. Three times you draw an orange ball. One time you draw a white ball. What is the new probability that there are  $n$  orange balls in urn, for each  $n = 0, \dots, 9$ ?

4. In the situation of the previous problem, determine the expected value of the number of orange balls in the urn.

5. Solve examples 2.10 and 2.11 on page 31 of MacKay.