Problem Set #1

CMSC/Math 456
Instructor: Daniel Gottesman

Due on Gradscope, Thursday, Sep. 7, noon (before start of class)

General instructions: You can solve these problems by hand or with the assistance of a computer, but in the latter case, you must write any relevant code yourself. If you collaborate or use any outside resources, remember to cite them in your solutions.

Problem #1. Decoding a Cipher with a Known Plaintext (60 points)

For this problem, you are Eve. You have been monitoring Alice and Bob, and you have determined that they are using substitution ciphers to communicate, but unfortunately, they change their key often and send only short messages, so you frequently have difficulty decoding their messages. You have also been watching their activities, which can sometimes give you clues to the contents of the messages. One day, Alice sends to Bob the message "XNNGX NHVGO NECDN RTGNT XRTJG NF" and then goes to meet Bob. You guess that Alice's message decrypts to "Meet me by the lake in ten minutes."

a) (20 points) Give any part of the key you can deduce assuming this is a correct decryption.

b) (20 points) Not long after their meeting, Bob sends Alice the message "GONHC TDCAA YJTGT JXHNB RFSRK NZNBY ZNBYG OBNNF RQSYJ BGPY." Do you think they are still using the same key as for the previous message? Why or why not?

c) (20 points) Decrypt as much of the second message (from part b) as you can.

Problem #2. Message Probabilities and Conditional Probabilities (60 points)

If you need a refresher on probability beyond what we did in class, see appendix A.3 of the textbook

For this problem, consider the encryption scheme given by the following table:

Message	$k = 0$	$k = 1$	$k = 2$
Today	cow	dog	horse
Tomorrow	dog	horse	pig
Next week	pig	cow	dog

The ciphertext is determined by the row corresponding to the message to be sent and the column corresponding to the value of the key. That is, if the message is "today" and the key $k = 0$, then the ciphertext is "cow," whereas if the message is "today" and the key $k = 1$, then the ciphertext is "dog."

Suppose Eve considers the messages "tomorrow" and "next week" to be twice as likely as "today," i.e.,

$$\Pr(M = \text{today}) = 1/5$$
$$\Pr(M = \text{tomorrow}) = 2/5$$
$$\Pr(M = \text{next week}) = 2/5.$$

All key values are equally likely.

a) (20 points) Calculate the probability $\Pr(C = c)$ of each possible value c of the ciphertext.

b) (20 points) Calculate the conditional probability $\Pr(C = \text{horse}|M = m)$ that the ciphertext is "horse" given each of the three possible messages m.

c) (20 points) If the ciphertext is “horse,” what is Eve’s conditional distribution $\Pr(M = m|C = \text{horse})$ for the three possible messages m?