HW 1 FEEDBACK

Dear Students,

Welcome to the class Making, Breaking Codes of Fall 2018! We hope you will find lots of fun in the class. We are pleased to see that most of you did the calculations correctly. Nonetheless, we have some comments during the grading for the first homework:

(1) We would like to point out that although this is not a proof-based class, the processes of making and breaking codes have to be **logical, rational and deductive**. That's why one shouldn't just write down answers without providing solid justification. You don't have to write long paragraphs as in the textbook, but at least you need a few **complete sentences**. Writing in words instead of using arrows pointing to these and that is so much clearer and is helpful for grading! Also, be precise, concise and organized. Quite a proportion of the class fails to do so in the first HW set.
(2) Sometimes you may want to use, e.g., tables, other than words to explain your answers. This is perfectly fine, but please tell us what are you doing in the table, what do the items in the tables mean etc. Don't just draw a table and then state the answer. This is not a complete explanation.
(3) Explain and define all of your notations!

In the following, let's give some examples on what do we expect.

Problem 10(b). You may write something like:

By part (a), the most probable key length is 2. We then divide the ciphertext into BBBAB and AAAAA. It is given that the letter b occurs much more frequently than the letter a. Therefore, the letters A and B should correspond to the letters a and b respectively in BBBAB; while the letter A should correspond to the letter b in AAAAA. We conclude that the key is (0,1), or ab. Using this key, the plaintext is bbbbbbabbb.

(It would be even better if you also compute the frequencies in the ciphertext and compare with the given frequencies.)

□

Problem 8 (a). First let's recall the question: 'Show that there are exactly eight possible choices for the integer α that allows you to decrypt.'

Many of you are able to find out these integers (the ones from 1 to 29 that are coprime to 30). This is an easy task. In fact, you can simply list them out without explaining too much. It is much more important for you to realize why coprimality is equivalent to being able to decrypt. You should elaborate on this.

A possible Ans for Q.8 (a) is:

The function $x \mapsto \alpha x + \beta \pmod{30}$ *is* ***one-to-one*** *if and only if* α *is coprime to* 30*. In this case, we will not have two letters being mapped to the same one. The possible choices of* α *are* $1, 7, 11, 13, 17, 19, 23, 29$*.*

□

Date: September 15, 2018.

Remark 0.1. For Q.11, if you compare the numbers of matches when shifting with length 1,2,3, they are not that far apart. That's why it would be better to compute also the frequencies in the ciphertext (after breaking up into groups according to the key length) and compare them with the provided frequencies of the problem. However, **no point** will be deducted if you did not do so because this is just an exercise for you to see how Vigenere method works.

In fact, similar comments for Q.10: if you also check for shift of 4, the number of matches is 5, which is also close to the number of matches of shift of 2.

Remark 0.2. The following is a very minor issue: please stick to the convention of the book:

(1) for plaintext, use lowercase letters
(2) for ciphertext, use uppercase letters.

The reason is that sometimes you want to use '=' to match the letters in plaintext and ciphertext (e.g., $A = a$)