CMPUT 299, Winter 2018, Assignment 1

Acknowledge **all** *resources consulted (discussions, texts, urls, etc.) in working on this assignment.* **Without this acknowledgement, your assignment will not be graded.** *Non-detailed oral discussion with others (including non-students) is permitted as long as any such discussion is summarized and acknowledged by all parties; the viewing or exchanging of any written work, even in rough or preliminary form, is expressly forbidden, as is any detailed discussion.* **Late assignments will not be accepted.**

As noted in chapter 8, the number of possible keys for the transposition cipher is equal to half the length of the message. This means that, unless the message is extremely long, it is still possible to use the brute force technique to decipher a message enciphered with the transposition cipher, even without the key. This exercise will guide you to implementing a stronger cipher, much more resistant to brute force attacks.

The transposition cipher enciphers a message by writing the message down in rows, and then reading of the columns, from left to right. For example, to encipher the message "CIPHERS ARE FUN" with key 5, we create the following table. We then read the columns left to right to get the ciphertext "CREIS P FHAUERN"

```
C I P H E
R S _ A R
E _ F U N
```

Instead of always reading the columns left to right, suppose we read the columns of in the order 4, 5, 3, 1, 2. We would get the ciphertext "HAUERNP FCREIS " (note the trailing space character). On the other hand, if we choose the order 2, 4, 1, 5, 3, we get the ciphertext "IS HAUCREERNP F". In fact, the number of orders in which we can read these five columns is 5!, which is equal to 120. Even if a hacker knows we used five columns in our table, they still wouldn't know which of the 120 possible orders will allow them to break the code.

Better still, the number of possible order increases very quickly with the number of columns, since the factorial function grows extremely fast. If we used ten columns instead of five, the number of possible orders is over three million. If we used fifteen, the number of orders is over one trillion. The brute force technique will fail as long as the number of columns is not too small.

Note that the key is no longer a single number, but a particular permutation of the numbers from 1 up to a particular number. For example, "2, 4, 1, 5, 3" is a possible key to this cipher. This modification – changing the key from a number to a permutation, and reading the columns in that order– results in the *columnar transposition cipher*.

To simplify the exercise, we will make one further modification to the transposition cipher: if the message length is not a multiple of of the length of the key, pad the end of the message with space characters. This avoids the need for "shaded boxes" in the decryption step, which will simplify this assignment.

You will produce five files for this assignment: four Python scripts (one for each of the four problems), and, for problem four, a file containing a decipherment of an enciphered text extracted from Wikipedia. For your submission, put all five of these files in a directory called 299-as-1. Zip this directory so that you have a new file called 299-as-1.zip. To submit the assignment, upload your zipped assignment to the assignment page in eClass.

Problem 1: Modify transpositionEncrypt.py so that it implements encryption using the columnar transposition cipher. Name the resulting Python file "a1p1.py". The "encryptMessage" function should take two parameters: the second is the message to be encrypted, as before, and the first, the key that determines the order in which the columns are read, should be a list of numbers containing 1 and every integer up to the length of the list. For example, encryptMessage([2,4,1,5,3], 'CIPHERS ARE FUN') should return 'IS HAUCREERNP F'.

Problem 2: Now that you can encrypt using the columnar transposition cipher, the next task is to be able to automatically decrypt. Modify transpositionDecrypt.py so that it implements decryption using the columnar transposition cipher. Name the file containing your code "a1p2.py".

To test your code, try decrypting the ciphertext "XOV EK HLYR NUCO HEEEWADCRETL CEEOACT KD", which was encrypted using the key [2,4,6,8,10,1,3,5,7,9].

Problem 3: At this point, you have Python modules which should be able to encrypt and decrypt with the columnar transposition cipher. The next step is to automate the testing of these modules.

Modify transpositionTest.py so that it tests the modules you wrote in problems 1 and 2. Name the file containing your code "a1p3.py". The program should still run tests on 20 random strings, generated the same way, and should still test all possible key lengths. For each key length, 10 random keys should be generated and tested.

Problem 4: Modify transpositionFilecipher.py to use the columnar transposition cipher. Name the file containing your code "a1p4.py". After testing your program, use it to decrypt the file "mystery.txt", which contains some text extracted from Wikipedia, encrypted using the columnar transposition cipher with the key [2,4,6,8,10,1,3,5,7,9]. The output should be saved in a file named "mystery.dec.txt", which should be included in your submission.