Homework #3

Due: May 21, 2014 **Points:** 100

A *transposition cipher* is a cipher that rearranges letters according to an agreed-upon pattern. For example, suppose we want to send our friend the secret message (called *plaintext*) `HELLOWORLD`. We can first write down every other letter, beginning with the first (`HLOOL`); do the same thing but beginning with the second letter (`ELWRD`); and then put them together (`HLOOLELWRD`). So we send our friend the enciphered message (called *ciphertext*) `HLOOLELWRD`.

When our friend receives it, she breaks the message in the middle: `HLOOL ELWRD`. She then writes down the first letter from each part (`HE`), the second letter from each part (`LL`), and continues until she has written down all the letters in that way (`OW OR LD`). She then puts them together to get `HELLOWORLD`, the actual plaintext.

This works well if the message has an even number of letters. But what if there are an odd number of letters? In this case, you just stop when there are no more letters. So, for example, the message `HITHERE` (7 letters) is enciphered as `HTEEIHR`. To decipher it, do as before, but when you divide the ciphertext into two parts, make the first part one letter longer than the second. So the two parts would be `HTEE` and `IHR`, and taking letters from each as before, the recipient gets the pairs `HI`, `TH`, `ER`, `E` (note the last one has just one letter). Putting them together gets the original plaintext, `HITHERE`.

Your goal is to write two programs, one that enciphers a message and prints the ciphertext, and the other that deciphers ciphertext and prints the plaintext, using this particular transposition cipher.

1. (*35 points*) Write a program to do the enciphering. It should prompt the user for a message, and print out both the entered message and its corresponding ciphertext.

   Input. The message to be enciphered. Here is what a correct input should look like (the red text is what you type):

   ```
   Enter your message: WHENINTHECOURSEOFHUMANEVENTS
   ```

   Output. The message to be enciphered and the corresponding ciphertext. Here is what the output corresponding to the above input should look like:

   ```
   plain = "WHENINTHECOURSEOFHUMANEVENTS"; cipher = "WEITEOREFUAEETHNNHCUSOHMNVNS"
   ```

   (note the double quotes around the plaintext and ciphertext).

   Here is another example. The input is:

   ```
   Enter your message: CALLMEISHMAEL
   ```

   and the corresponding output is:

   ```
   plain = "CALLMEISHMAEL"; cipher = "CLMIHALALESME"
   ```

   Submit. Name your file "encipher.py" and submit it to the Homework #3 area for this class on SmartSite.

2. (*35 points*) Now write a program to decipher the messages. Again, it should prompt the user for a ciphertext, and print out both the entered ciphertext and the corresponding plaintext.

   Input. The message to be deciphered. Here is what a correct input should look like (the red text is what you type):

   ```
   Enter your ciphertext: WEITEOREFUAEETHNNHCUSOHMNVNS
   ```

Output. The message to be deciphered and the corresponding plaintext. Here is what the output corresponding to the above input should look like:

```
cipher = "WEITEOREFUAEETHNNHCUSOHMNVNS"; plain = "WHENINTHECOURSEOFHUMANEVENTS"
```

(note the double quotes around the ciphertext and plaintext).

Here is another example. The input is:

```
Enter your ciphertext: CLMIHALALESME
```

and the corresponding output is:

```
cipher = "CLMIHALALESME"; plain = "CALLMEISHMAEL"
```

Submit. Name your file "decipher.py" and submit it to the Homework #3 area for this class on SmartSite.

3. (*30 points*) Now we will combine the two parts you just did into a single program. This program asks the user to type 'e' to encipher or 'd' to decipher. If the user asks to encipher, the steps in the first part are to be followed; if to decipher, the steps in the second part are to be followed.

   Input. Whether the message is plaintext and is to be enciphered, or whether the message is ciphertext and is to be deciphered, followed by the message. Here is what a correct input should look like (the red text is what you type):

   ```
   e to encrypt, d to decrypt): e
   Enter your message: WHENINTHECOURSEOFHUMANEVENTS
   ```

   Your program must be able to handle either an 'e' (lower case) or 'E' (upper case) to indicate enciphering, and either a 'd' or a 'D' to indicate deciphering.

   Output. The entered message and the corresponding ciphertext or plaintext. Here is what the output corresponding to the above input should look like:

   ```
   plain = "WHENINTHECOURSEOFHUMANEVENTS"; cipher = "WEITEOREFUAEETHNNHCUSOHMNVNS"
   ```

   (note the double quotes around the plaintext and ciphertext).

   Here is another example. The input is:

   ```
   e to encrypt, d to decrypt): D
   Enter your ciphertext: CLMIHALALESME
   ```

   and the corresponding output is:

   ```
   cipher = "CLMIHALALESME"; plain = "CALLMEISHMAEL"
   ```

   Submit. Name your file "combined.py" and submit it to the Homework #3 area for this class on SmartSite.