Homework 1: Warmup

Submission policy. This assignment is due **typed** as a **PDF** on **Wednesday, January 28, 2015** at **11:59PM** via websubmit. Late submissions will be penalized according to course policy. Your writeup MUST include the following information:

1. List of collaborators (on all parts of the project, not just the writeup)
2. List of references used (online material, course nodes, textbooks, wikipedia, etc.)
3. Number of late days used on this assignment
4. Total number of late days used thus far in the entire semester

If any of this information is missing, at least 20% of the points for the assignment will automatically be deducted from your assignment. See also discussion on plagiarism and the collaboration policy on the course syllabus.

Adminstration. This assignment will be administered by Aanchal Malhotra.

Exercise 1. The following text was encrypted with a substitution cipher. (Spaces and punctuation marks were preserved from the plaintext.)

```
THVVWCZTQ!
CZ WECQ YIAQQ, LFN JCII IVAHZ WEV DCPPVHVZYV MVWJVVZ VZYHLOWCFZ AZD ANWEVZWCYAWCFZ.
WECQ RVQQATV CQ VZYHLOWVD JCWE A BVHL CZQVYNHV VZYHLOWCFZ QYEVRV. CDVAIIL, AZ
VZYHLOWCFZ QYEVRV QEFNID AIIFJ FZIL ANWEFHCGVD OAHWCVQ, JEF XZFJ WEV XVL, WF HVAD
WEV RVQQATV. EFJVBVH, LFN SNQW HVAD WEV RVQQATV JCWEFNW XZFJCZT WEV XVL. EVZYV,
WEV VZYHLOWCFZ QYEVRV CQ CZQVYNHV.
```

Find the plaintext. Feel free to do this by hand, or with a computer program. You can find tables of English letter frequencies on the web.

Exercise 2. The one-time pad is a long sequence of random letters. These letters are combined with the plaintext message to produce the ciphertext. To decipher the message, a person must have a copy of the one-time pad to reverse the process. A one-time pad should be used only once (hence the name) and then destroyed. This is the first and only encryption algorithm that has been proven to be unbreakable.

To encipher a message, you take the first letter in the plaintext message and “add" it to the letter from the one-time pad. To decipher a message, you take the ciphertext and “subtract” the letter from the one-time pad. By “adding”, we mean the following:

Let A be the 0th letter in the alphabet. ... Let Z be the 25th letter in the alphabet. To "add" letter S (the 18th letter) and C (the 2nd letter), take:

$$18 + 2 \mod 26 = 20$$

which gives us U (the 20th letter). To "subtract" letter U (the 20th letter) and C (the 2nd letter), take:

$$20 - 2 \mod 26 = 18$$

which gives us S (the 18th letter).
Here's a larger example:

plaintext	SECRETMESSAGE
one-time pad	CIJTHUUHMLFRU
ciphertext	UMLKLNGLEDFXY

Dr. X was not paying attention in her security class, and decided to reuse the same 5-letter "one-time pad" over and over to encipher her plaintext. The result is shown below. (We've retained the punctuation in the message to make codebreaking easier for you.)

```
Z LUNI R HLWED XBSX FRY VEP XBAW EENASE ACDP IMMW YG EHV PZZY GYK XBW XIYY EIRRCFK
FJ CLW TVYWH: "NI BGPU XBWWV XLMXYW NG FV WYDJ VZCVIEX, NZEK EFD QVR UJI TVYSXVH
YIYRP." -GDO
```

Write a python program that allows you decipher the message below, which is also enciphered using the same 5-letter "one-time-pad". We have not retained the punctuation for the message below.

```
ZPINIGMTRE.
```

Submit your python program and the deciphered message. You can use whatever decipherment technique you want; feel free to read online to find ideas! (Just make sure to cite your sources!)

NOTE: It turns out that this way of repeating the use of a "one-time pad" is also known as a Vigenère cipher, after Blaise de Vigenere, who published his description of the cipher before the court of Henry III of France, in 1586. It has been used throughout history. For example, the Confederate States of America used the Vigenere cipher during the American Civil War. The Confederacy's messages were far from secret and the Union regularly cracked their messages. Throughout the war, the Confederate leadership primarily relied upon three key phrases as their "key": "Manchester Bluff", "Complete Victory" and, as the war came to a close, "Come Retribution".