Submit <u>one</u> zip or rar file named as yourlastname_yourfirstname_HillCipher. It should include the following files:

- Source code in one file as a .c, .cpp or a .java
- A report on your assignment (will send an announcement regarding the details about the report on or before 6/10/14)

CIS 3360 – Security in Computing
Summer 2014
Programming Assignment (100 points)

In this assignment you'll write a program that encrypts the alphabetic letters in a file using the Hill cipher. Your program should prompt the user for the names of two input files and one output file:

1) The file storing the encryption key
2) The file to be encrypted
3) The corresponding encrypted file

Your program should open the first two files, make the necessary calculations and write the ciphertext to the third file.

If the file to be encrypted doesn't have the proper number of alphabetic characters, pad the last block as necessary with the letter 'X'.

<u>Encryption Key File Format</u>

The encryption key file will store a single positive integer, n *(1 < n < 10)*, on the first line, indicating the number of rows and columns in the encryption matrix. The following n lines will contain the contents of each row, in order, of the encryption matrix, separated by spaces.

<u>Format of the File to be Encrypted</u>

The file to be encrypted can be any valid text file with no more than 9991 letters in it. (Thus, it's safe to store all characters in the file in a character array of size 10000, including any padding characters.)

<u>Format of the File storing the Ciphertext</u>

Each line of output should have exactly 80 lowercase letters on it, except for the the last row (possibly). These characters should correspond to the ciphertext of encrypting all the letters in the input file.

<u>What to Turn In over WebCourses</u>

Turn in a single file***, hill.c*** or ***hill.java*** storing your solution to the problem.

<u>Program Notes and Hints</u>

You must read in a file that contains uppercase letters, lowercase letters and non-letter characters. Your program must distinguish between these three groups so that what gets encrypted is always a lowercase character and the output should always be a lowercase character. All non-letter characters in the file are simply skipped and not counted as part of the plaintext.
One possible breakdown to solve this problem is as follows:
1) Write a section of code or function that reads in the input file into an char array of size 10000, storing only the appropriate lowercase letters in the character array.

2) Write a section of code or function that takes as input the array from section 1 and the encryption key and produces an array of ciphertext storing only lowercase letters.

3) Write a section of code or function that takes as input the array storing the ciphertext and outputs it to the output file in the format specified.

Sample Key File

```
3
1 1 6
3 3 1
5 2 7
```

Sample Input File

```
CS: the science that deals with the theory and methods of processing information in
digital computers, the design of computer hardware and software, and the
applications of computers.

IT: the development, implementation, and maintenance of
computer hardware and software systems to organize and communicate information
electronically. Abbreviation:  IT

Computers are man-made tools that aid us in solving other problems. A biologist is
trying to figure out how life works, physicists and chemists are trying to figure out
how items react in our universe, mathematicians are trying to figure out rules for
man-made systems.

Any research problem that may improve a computer's capability of helping solve a
problem or any research problem that sheds light about a new way to do something with
a computer is part of CS.

Most exciting research: Medical Applications (Expert Systems for Diagnosis,
Remote surgery, nano-devices with computing power to deliver medicine, etc.),
We need help trying to create a comprehensive EMR accessible to the right people only,
Cars that can drive themselves – seems like the best way we know how to solve lots of
problems is by throwing lots of computing power at them, instead of looking for
elegant solutions. This doesn't sound exciting, but it will be exciting when the
results are achieved. (ie Watson)

CS students tend to find jobs where they program at least some.
In the process, they are solving problems.
Challenges: It's impossible to teach all the new languages/toys.
Ultimately, we just need to teach our students how to think, so that they can pick up
new things on their own. Our biggest challenge is getting them to buy into that.

Ethical: Lots, with security etc.
```

Corresponding Output File

```
ebxpzniicnxtaafuszpzsofzqhsnydqtlyhdnxpgozbztszsoaygmapndyqrdjfhrbvyqvnvbdatbbrx
wviobovfzckgsfiykistuolszjcdufvezhbztaqjpdkfqvyehbiffhhpnqfvofhqmprlrkfjvcrafzcn
iixvcbsxgxnjfrbsxpnqbdskizildxemzpowhfkistuolszjcdufvezhbztaqjpdkuoerdfrvspvqjve
djdcyhumwddamznmxxrwqwdlwbdnxstclxlwqrjjbzaxwvfopnqxlwbzprxwvioqtbqwszxlroaqrtbo
vtfmbbeanpudndweebjjygmgzkodemsppjdvktbktblbhdycpngyrhiwggozddglxfnzsxcnmeeowwl
hbcyhftxktbqtbvivgftflkxtfjlgsrjxhjzhccdhqoibqugpvddaxoyqaajmjqwsnfvilbqtbvivgft
flkxtfjlgsrjzsuatnzbghzgbniuoerdfspznxawoujmimgzkodvwrnrsucazubhfkiuyrxwviouiqvu
epnoxnhkopwilxxvvsfqbvlqqjfrfpajyyusgdbwufcdetapvromxbcjwyexxzgysrjlrcscyxnwvrny
eswijvbxrkxiuyrxwviompzbslfhqkaejlavftbquvvowoujmiizlkesxwewixmznwbdelzrwuzfnjla
irbxsvseefvlyrnwkmbjvvnujjonaapdaplfykcrkxkistuofreffxfefpdapakpxiddekrnsrfwyepd
xiifktklbhdyconlofxqoimprlsmvrqbngonhoisagaxmpdfayehjdnmpwerxvhfmsvaxzbovfhafqvv
sonyduoolohagackizrmyjjriyghhkmsikgdznxhjlnpvsfvhkrvvszsdetuoogbfhgzhlhfrejqikxx
kistuofreffxvlccramewpiawpphqbkqmfrerwqnxsgfrrvvpiuwbdbovsdtwuwkkviltpscuxdfrefe
wdzyhqjdtpvftbqusntbsxjygmioielpdksnbifnddeaamrvvtlnbbihikvaejcplacnojdscexbtpey
ehlejsztmkycqpcvnaeumxxyehmgzkkobovcgqzdlvsffremgzkodqogvgipgyowifvwgxnkkyxmpdfa
xrzjbyghclueollxtqeomghhqckpivuimlcysmkhbdewtrodfzgsnbgpvbbihikboyuxnxcbdvgqlrro
myehaauyovceoakzfapfregfbyehflqpparilywqghhjbyusbrjbkgohkjfreyehldojjfferxcbrjow
ijqrjjqikyiesbwmijqamzbhuj
```

Sample Program Run (User input in bold)

```
Please enter the name of the file storing the key.
samplekey.txt
Please enter the name of the file to encrypt.
panelnotes.txt
Please enter the name of the file to store the ciphertext.
panelnotes-enc.txt
```