

CS1132 Fall 2015 Assignment 2 due 11/19 11:59pm

Adhere to the Code of Academic Integrity. You may discuss background issues and general strategies with others and seek help from course staff, but the implementations that you submit must be your own. In particular, you may discuss general ideas with others but you may not work out the detailed solutions with others. It is never OK for you to see or hear another student's code and it is never OK to copy code from published/Internet sources. If you feel that you cannot complete the assignment on your own, seek help from the course staff.

When submitting your assignment, follow the instructions summarized in Section 4 of this document.

Do not use the `break` or `continue` statement in any homework or test in CS1132.

Do not use the built-in functions `find`, `strfind`, or `findstr`.

1 Cryptography Fun!

Not long ago, cryptography existed solely in the domain of national governments and large corporations. However, the advent of the Internet and the broad availability of computers have now made cryptography an indispensable part of everyday digital communications. In this part of the assignment, you will implement one well-known classical cipher, the Vigenere cipher. This cipher predates modern cryptography but nonetheless provide a relevant and insightful look at some basic cryptographic principles. You will implement this cipher as MATLAB functions that can be used to encrypt and subsequently decrypt messages.

The Vigenre cipher is one of the most well-known ciphers of all time. It is a method of encrypting plaintext using a series of different Caesar ciphers based on the letters of a key (keyword). The Vigenre cipher can be implemented using what is called a tabula recta, or Vigenre square. It consists of the alphabet written out 26 times in different rows with each row consisting of the alphabet shifted cyclically to the left. The Vigenre square is shown below ¹:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 1: Vigenre square

¹<http://en.wikipedia.org/wiki/Vigen%C3%A8recipher>

For example, the plaintext MATLABISFUN when encrypted using the key CIPHER, gives the ciphertext OIISESKAUBR. The encryption works by first taking the key and repeating it till it matches the length of the plaintext. Subsequently, each character in the plaintext is paired with the character in the key in the corresponding position. The characters of the plaintext correspond to the columns of the Vigenre square and the characters of the key correspond to the rows. For instance, using the example below, the first letter of the plaintext M is paired with the first letter of the key C. The row C and column M of the Vigenre square gives the letter O. This is repeated for the rest of the letters in the plaintext.

```
Plaintext:  MATLABISFUN
Key:       CIPHERCIPHE
Ciphertext: OIISESKAUBR
```

For the purpose of the assignment, we simplify the implementation of the cipher by allowing the plaintext (and ciphertext) to contain only uppercase letters with no other punctuations, whitespaces or symbols. If the user were to enter invalid characters, the function should remove them. If the user were to enter lowercase letters, they should be converted to uppercase. For example, if the input is MATLAB is fun!, it should be converted to MATLABISFUN.

Additionally, the function that you implement, when given the correct key, should be capable of decrypting any ciphertext that was encrypted using the Vigenre cipher. A parameter in the function is used to indicate which mode the function is in: encryption or decryption.

Write a function to implement the Vigenre cipher as described above:

```
function output = vigenere(instr, key, encdec)
% Encryption and decryption using the Vigenere cipher
% instr: Plaintext to be encrypted or ciphertext to be decrypted, a string
% key: key to be used in encryption, a string
% encdec: 0 means encrypt and 1 means decrypt; assume that encdec is always 0 or 1
% output: ciphertext when encrypting; plaintext when decrypting; a string
```

2 Single Vowel in Dictionary

A subset of words and phrases from a dictionary has been scrambled and is stored in no apparent order in the text file *randPermDic.txt*. Fortunately, each word/phrase has a rank (entry number) from the dictionary that has been retained in the file. Below are the first few lines from the file:

```
45057, laudanum
24653, common room
23755, clerestory
71146, unrestrained
```

Write a program to read *randPermDic.txt*, identify the words/phrases that contain just a single vowel, sort those words/phrases by their dictionary rank, and write them to a plain text file in sorted order. Below are the requirements for your solution:

- Implement this function to solve the problem:

```
function n = sortDicWithSingleVowel(dicName, sortedDicName)
% dicName names the file that contains words/phrases in scrambled order.
% Identify the words/phrases that contain a single vowel,
% sort them in ascending order by the word/phrase rank, and write them in
% sorted order to a plain text file.
```

```

% n is the number of lines written to the output file.
% sortedDicName names the output file to be written.
% Eg., n=sortDicWithSingleVowel('randPermDic.txt','sortedDicWithSingleVowel.txt')

```

- Use a cell array to store the string data from the file. The word/phrase on the first line of the file should be stored in the first cell of the cell array, the word/phrase of the second line of the data file should be stored in the second cell of the cell array, and so forth. The cell array should be just big enough to store the data; there should not be any empty cells. Store the ranks in a corresponding fashion but use a simple array (so that you can later sort the ranks easily).
- Use only the letters 'a', 'e', 'i', 'o', and 'u' as vowels (include both upper and lower case). Filter the original cell array to store the words/phrases with just a single vowel in a new cell array. Correspondingly you need to keep track of the ranks.
- Use subfunctions! For example, a subfunction that checks if one string contains only a single vowel is super useful.
- Use Matlab built-in function `sort` to sort the ranks. Sort in ascending order. (Type `help sort` in the Command Window to learn about `sort`.)
- Write the words/phrases that contains only a single vowel, including their rank, in sorted order in a plain text file. Part of the resulting file should look like this:

```

2050,Born
2058,Bors
2060,Bosch
2106,Boyd
2110,Boz
2120,Bragg
2132,Brahms
2139,Brandt

```

Below is a list of useful built-in functions for handling characters, strings, and files. Use only these built-in functions for handling characters, strings, and files. You may not need all of them. You can of course still use general built-in functions not related specifically to strings and files, such as `length`, `zeros`, `rem`,... etc.

You can use:

- `fopen`, `feof`, `fgetl`, `fclose`
- `strcmp`, `upper`, `isspace`, `isletter`, `str2num`

Function `str2num` converts a string representing a number to the numeric value. For example: `str2num('0035')` returns the numeric scalar 35.

3 Graphics Fun!

In this part you will implement `Minesweeper` using Matlab's graphics functions. For our game, we will consider an $n \times n$ board with m mines randomly distributed among the squares on the board.

Initially, all the squares on the board are covered. The goal of the game is to mark all the mines and uncover all the squares that do not contain mines. During the game, the player uses a left click to uncover a square (that hopefully doesn't contain a mine) and a right click to indicate a mine.

With this exercise, you have the freedom to structure the code as you see fit. You should define helper functions as needed to make your solution modular—do not submit one long giant function. The helper functions, i.e., subfunctions, must be saved in the same file containing the main function for the game: `minesweeper.m`. The function takes as input arguments n and m , the dimension of the board and the number of mines, respectively. For scaling purposes, you may assume that n is an integer between 5 and 20. Also, you should make sure that $0 < m < n^2$. Here are the requirements:

- The interaction happens only in one figure window.
- Display the $n \times n$ board in the figure window and the name of the game as the title of the figure
- Pick the location of the m mines randomly with equal probability, i.e., each square on the board is equally likely to have a mine.
- The player can left or right click on a square on the game board. Use the Matlab built-in function `ginput` with a third output parameter to get the button identifier in addition to the coordinates of the user's click. E.g., `[x,y,button] = ginput(1)` returns the x-coordinate, the y-coordinate, and the button or key designation for one click. `button` is an integer indicating which button was used: 1 for left, 2 for middle, 3 for right. In our game, you can assume that the player never middle clicks.
- Player clicks on a square that is covered (has not been clicked before): A right click marks the square as a mine and the program should put an X on the square, regardless of whether it really is a mine. A left click ends the game with the player losing if the square contains a mine; otherwise the color of the square is changed and the number of neighboring mines (a number between 0 and 8) is displayed on the square.
- Player clicks on a square that is marked by a number: Prompt the user (using the title of the figure) to click another square.
- Player clicks on a square that is marked by an X : A right click does not change the state of the square. Prompt the user to click another square. A left click ends the game with the player losing if the square contains a mine; otherwise the color of the square is changed and the number of neighboring mines is displayed on the square.
- If the player loses (left clicks on a mine), the game must not allow another click. Display a message as the figure title saying that the player has lost and then end the game.
- The player wins the game when all the mines are marked with X and all the empty space are marked with numbers. Display a congratulatory message as the figure title and then end the game.
- If all the squares have been marked but the player has not won (there are more X marks than mines), the game continues—keeps accepting another click.

4 Self-check list

The following is a list of the minimum *necessary* criteria that your assignment must meet in order to be considered *satisfactory*. Failure to satisfy any of these conditions will result in an immediate

request to resubmit your assignment. Save yourself and the graders time and effort by going over it before submitting your assignment for the first time. Although all these criteria are necessary, meeting all of them might still not be *sufficient* to consider your submission satisfactory. We cannot list everything that could be possibly wrong with any particular assignment!

- △ Comment your code! Make sure your functions are properly commented, regarding function purpose and input/output parameters.
- △ Suppress all unnecessary output by placing semicolons (;) appropriately. At the same time, make sure that all output that your program intentionally produces is formatted in a user-friendly way.
- △ Make sure your functions names are *exactly* the ones we have specified, *including* case.
- △ Check that the number and order of input and output parameters for each of the functions match exactly the specifications we have given.
- △ Test each one of your functions independently, whenever possible, or write short scripts to test them.
- △ Check that your scripts do not crash (i.e., end unexpectedly with an error message) or run into infinite loops. Check your script several times in a row. Before each test run, type the commands `clear all; close all;` to delete all variables in the workspace and close all figure windows.

5 Submission instructions

1. Upload files `vigenere.m`, `sortDicWithSingleVowel.m`, and `minesweeper.m` to CMS in the submission area corresponding to Assignment 1a in CMS before the deadline. Late submission is accepted up to 24 hours after the deadline with a 10% penalty.
2. *After grading:* If you resubmit the assignment, upload your corrected files and *be sure to select the **Regrade Request** option.*