AP Computer Science Name _____

Final Exam Project: Cryptography

The following test is due on or before Friday, May 26th, 2017 **end of school (3:00 P.M.)**.
It will not be accepted after this time. Note: if you cannot find me, you may submit this sheet to my mailbox in room 702 by the deadline. Mrs. Sampson may assist you if you need it.

This test is to be done independently, without the aid of websites, knowledgeable acquaintances and classmates or any other aid that would not be available during a normal in-class exam. The one exception is consulting the Java API for reference. There is no time limit on the exam, only the condition that once you open the exam you do not consult any of the above-disallowed references.

Hereunder I sign that I've read these conditions and will abide by them. I understand that Mr. Harris will grade the exam fairly. I also understand that Mr. Harris finds academic dishonesty increasing, and totally reprehensible as well as personally insulting.

Signed:_____

AP Computer Science
Final Exam Project: Cryptography

Objective: To design and implement a complete software solution with an appropriate and efficient data structure including all of your current programming knowledge.

Program Description: During all the major wars and conflicts, maintaining secrecy was a top priority for both sides. Having a strong encryption or cipher allowed communication to continue between the various leaders within each side without the fear of that valuable information be discovered by the opposition. Your task will be to write a classic cipher algorithm and it's complimentary decipher code along with a complete program that demonstrates all of it's features.

The Cipher: The Myszkowski Transposition Cipher is a columnar technique for encrypting a plaintext document, proposed by Émile Victor Théodore Myszkowski in 1902. The methodology: plaintext is written out in rows under a keyword. When there are repeated letters in the keyword, rather than number them from left to right, you give all the same letters the same number. You then read across columns which have the same number in the keyword.

Encryption:

1. Choose a keyword to build your grid. Duplicate letters are good for improved encryption.
2. Create a grid with the number of columns matching the number of keyword letters.
3. Number each letter in the keyword with its alphabetical position, giving repeated letters the same numbers.
4. Write out the plaintext in the grid. Left to right , top to bottom.
5. Starting at number 1 (the first letter alphabetically in the keyword), and if it is the only appearance of 1, we read down the column. If, however, the number 1 appears more than once, we read from left to right all the first letters of the columns headed by 1. Then we move to the next row, and read across, left to right, the letters in the rows headed by 1. Once complete, we move on to the number 2, and so on. Until a complete encrypted text is created.

Example:

Given the following phrase -

"Begin at the beginning," the King said, very gravely,
"and go on till you come to the end: then stop."

Step 1: choose a keyword to build your grid. Let's use the word *brillig*

Step 2: create the grid

- place keyword at top (row 1)
- order the letters (row 2)
  duplicates go left to right
- type in your text to be encrypted left to right
  top to bottom.
- use all lowercase or all uppercase
- omit punctuation, spaces and nulls
- fill any remaining squares with an x

Step 3: write out the encrypted message:

b	**r**	**i**	**l**	**l**	**i**	**g**
1	*5*	*3*	*4*	*4*	*3*	*2*
b	e	g	i	n	a	t
t	h	e	b	e	g	i
n	n	i	n	g	t	h
e	k	i	n	g	s	a
i	d	v	e	r	y	g
r	a	v	e	l	y	a
n	d	g	o	o	n	t
i	l	l	y	o	u	c
o	m	e	t	o	t	h
e	e	n	d	t	h	e
n	s	t	o	p	x	x

btneirnioentihagatchexgaegitisvyvygnluetnhtxinbengngerelooyotodtopehnkdadlmes

For enhanced security you could repeat this process again with another keyword. But enough for now.

AP Computer Science Name _____

Final Exam Project: Cryptography

Decryption:

Step 1: write the keyword in your grid, top row. Reminder, we are using the word *brillig*

Step 2: order the letters (row 1)

Step 3: divide the length of the ciphertext by the length of the keyword to work out how many rows we need to add to our grid. We then have to systematically put the ciphertext back in to the grid.

Step 4: start at number 1, and continue to the highest number. If the number only appears once, we fill down the column. If the number appears twice, we move from left to right across the columns with that number heading them.

Step 5: now we read off the plaintext by reading across one row at a time, inserting spaces as needed.

Preplanning requirement:

Given the time constraint I am requiring you to do a little thinking before coding. On the back of the cover please hand write out your plan of attack. What data structure will you use, how will you handle the encryption and decryption. This should not be any code, only a bunch of notes as to the files and methods you may need to write and what they do.

Program Details:

- The program should contain a repeating menu with the following features:
    - Encryption
        - Create a keyword and save to text file
        - Load a keyword from a prompted filename
        - Enter text to encrypt and save to a file
            - create and display the grid, encrypt the text, and save the result to file
        - Load a file with text to encrypt and save
            - create and display the grid, encrypt the text, and save the result to file
    - Decryption
        - Create a keyword and save to text file
        - Load a keyword from a prompted file
        - Enter text to decrypt and save to a file
            - create and display the grid, decrypt the text, and save the result to file
        - Load a file with text to decrypt and save
            - create and display the grid, decrypt the text, and save the result to file
    - Exit the program.
- Multiple Classes and files should be used to solve this programming assignment.
- The text may include upper and lowercase letters, punctuation and digits.

Realize that I am attempting to ascertain what you have learned in this course, and how you handle the above scenario. Please do your best.

Submissions for the exam should include:

1. The ***original*** attached cover sheet, signed and with your preplanning on the reverse side.
2. This assignment sheet stapled to the above
3. Your electronic submission of all the required files .zip'd together and emailed to *harris@lexingtonma.org*

AP Computer Science
Final Exam Project: Cryptography

AP Computer Science
Final Exam Project: Cryptography

Name _____

Scoring Rubric

Concept	*Points*	
Paperwork Submitted	5	
Preplanning exercise	5	
Encryption		
Reading key and text from file	8	
User input of key and text	7	
Encrypting / Display	10	
Writing key and text to text file	7	
Decryption		
Reading key and text from file	8	
User input of key and text	7	
Decrypting / Display	10	
Writing key and text to text file	7	
Grid Key and data treatment	6	
Menu - repeating	5	
Compiles and Runs	5	
On-time Submission	10	
Total	100	

Scoring Rubric

Concept	*Points*	
Paperwork Submitted	5	
Preplanning exercise	5	
Encryption		
Reading key and text from file	8	
User input of key and text	7	
Encrypting / Display	10	
Writing key and text to text file	7	
Decryption		
Reading key and text from file	8	
User input of key and text	7	
Decrypting / Display	10	
Writing key and text to text file	7	
Grid Key and data treatment	6	
Menu - repeating	5	
Compiles and Runs	5	
On-time Submission	10	
Total	100	