Programming Languages

Homework – III

Deadline – 12.11.2014 before 13:00

In this homework, you will be implementing a playfair chiper, which is is a manual symmetric encryption technique and was the first literal digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair who promoted the use of the cipher.

The Playfair cipher uses a 5 by 5 table containing a key word or phrase.To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order (usually omitting "Q" to reduce the alphabet to fit; other versions put both "I" and "J" in the same space). The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. The keyword together with the conventions for filling in the 5 by 5 table constitute the cipher key.

To encrypt a message, one would break the message into digraphs (groups of 2 letters) such that, for example, "HelloWorld" becomes "HE LL OW OR LD", and map them out on the key table. If needed, append a "Z" to complete the final digraph. The two letters of the digraph are considered as the opposite corners of a rectangle in the key table. Note the relative position of the corners of this rectangle. Then apply the following 4 rules, in order, to each pair of letters in the plaintext:

1. If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Playfair use "Q" instead of "X", but any uncommon monograph will do.
2. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
3. If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
4. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.

To decrypt, use the INVERSE (opposite) of the last 3 rules, and the 1st as-is (dropping any extra "X"s (or "Q"s) that do not make sense in the final message when finished).

YOU CAN FIND MORE DETAILS on Playfair cipher by **READING** this link

http://en.wikipedia.org/wiki/Playfair_cipher

IMPORTANT - Your program will ask for a keyword and a string (a plain text) from user. Your program should create a 5x5 table from the keyword and then encrypt the plain text with Playfair cipher and finally print the 5x5 table and encrypted string on the screen.

WHAT TO SUBMIT

Your homework must include the following items:

1) A word document with a cover page, which has the name of the course, homework number, your student number, your name. Also a short description of your solution must be included in this document.

2) Source code of your program.

- **Please note that your code should include neccesarry comments**
- **Output of your source code must be in a readable form !!!**

3) Example program output (screenshot in jpeg or png format)

HOWTO SUBMIT

- You should e-mail the electronic versions of the above documents to my e-mail address (ziyacihantaysi@gmail.com) **before the DEADLINE!!!**
- Subject of your e-mail must include your student number and homework number as shown below;
  - **08011001 – HW1**
- Please do **NOT** include any executable (exe, bat, com, etc.) or archive files (rar, tar, zip, etc.) files among the attachments of your e-mail.