ITEC 4300

Mini Project 1: Encryption/Decryption

In this lab, you are going to work as a team to solve the playfair cipher encryption/decryption algorithm. Your team is required to design and develop a fully user interactive Playfair crypto system implemented in Java. The user will be able to input a plaintext in English and a keyword and the algorithm will produce the ciphertext. The use of any external Java libraries is prohibited in this work.

Playfair Cipher

The Playfair cipher encrypts pairs of letters (digraphs), instead of single letters. This is significantly harder to break since the frequency analysis used for simple substitution ciphers is considerably more difficult.

Memorization of the keyword and 4 simple rules is all that is required to create the 5 by 5 table and use the cipher.

```
KEYWO
RDABC
FGHIJ
LMNPS
TÜVXZ
```

The Playfair cipher uses a 5 by 5 table containing a key word or phrase. To generate the table, one would first fill in the spaces of 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 (to reduce the alphabet to fit you can either omit "Q" or replace "J" with "I"). In the example to the right, the keyword is "keyword".

To encrypt a message, one would break the message into groups of 2 letters. If there is a dangling letter at the end, we add an X. For example, "Secret Message" becomes "SE CR ET ME SS AG EX". We now take each group and find them out on the table. Noticing the location of the two letters in the table, we apply the following rules, in order.

1. If both letters are the same, add an X between them. Encrypt the new pair, re-pair the remaining letters and continue.
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 necessary. For example, using the table above, the letter pair GJ would be encoded as HF.
3. If the letters appear on the same column of your table, replace them with the letters immediately below, wrapping around to the top if necessary. For example, using the table above, the letter pair MD would be encoded as UG.
4. If the letters are on different rows and columns, 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 pair should be replaced first. For example, using the table above, the letter pair EB would be encoded as WD.

To decipher, ignore rule 1. In rules 2 and 3 shift up and left instead of down and right. Rule 4 remains the same. Once you are done, drop any extra Xs that don't make sense in the final message and locate any missing Qs or any Is that should be Js.

Teams: