Colin Salvato
Professor Arias
Software Development I
2/17/17

Playfair Cipher Encryption 

For project 2, I started off by choosing to create a simple file encryption software that would encrypt and decrypt files. After a lot of contemplation I found this idea to be a bit mundane and common. In my research about file encryption, I came across many different types of encryptions, like ciphers. A cipher is defined as a secret way of writing, very similar to file encryption. That's when I came up with the idea of writing a program that would cipher and decipher code. After a bit of research about ciphers and how they worked, I found the perfect type of hidden code that I could make in Java to cipher and decipher. This cipher is called the “Playfair Square” or the “Playfair Cipher.” It is a type of code that follows many types of rules that could be implemented into a piece of software in Java.

The way it works is a short keyword without any repeating letters is put into a five by five square. Then the rest of the alphabet is put into the rest of the five by five square (i and j are both put into the same letter). Then the first two letters of the word being encrypted is looked at on the five by five chart and depending on the position of the two letters on the chart in relation to each other, something happens:

Scenario 1: If the two letters are are in the same row as each other then the first two letters are encrypted as the letters to their right. If either of the letters are on the right of the row then you continue to the other side of the row.

Scenario 2: If they are in the same column then they are encrypted as the letter below them. If either of the letters are at the bottom of the column then you continue to the top of the column.

Scenario 3: If the two letters are not in the same row or column then an “imaginary” box is formed around the two letters with each of them in opposite corners, and the encrypted letters are the ones in the other 2 corners of the “box.”

This process is repeated until there are no more sets of letters to encrypt in the word being encrypted. The decryption process is nearly identical, it is just done in reverse. My program would ask the user for a keyword to create a five by five grid of letters and then ask the user if they would like to cipher or decipher a set of letters then it would spit out the set of ciphered/deciphered set of letters that the user asked for.

My program to implement all these features would be very manageable yet challenging for me. With the use of if statements, loops, and different methods, this program wouldn’t prove to be too difficult for me.