CRYPTOGRAPHY HANDOUT 04

PLAYFAIR CIPHER

The following will walk you through a Playfair Cipher example. Recall that the Playfair cipher uses a 5×5 grid to encrypt a message.

1. Encrypting Using Playfair

1. Choose a key word (no longer than 8 letters for now).

2. Write these in the following 5×5 grid. Keep in mind $i = j$. Then fill in the rest of the grid/matrix with the rest of the letters in the alphabet (no repeated letters and in alphabetical order):

3. Write a one-line message:

4. Remove spaces and punctuation. Divide the text into groups of two letters. Add an extra x at the end of the final group, if necessary.

5. Encrypt your message using the following rules:
   a. If 2 letters are not in the same row or column, replace each letter by the letter that is in its row and is in the column of the other letter.

   b. If 2 letters are in the same row, replace each letter with the letter immediately to its right, with the grid/matrix wrapping around from the last column to the first.

   c. If 2 letters are in the same column, replace each letter with the letter immediately below it, with the grid/matrix wrapping around from the last row to the first.

6. You're now going to give another group your encrypted message. Recopy your 5×5 grid/matrix on the provided paper, and also recopy your encrypted ciphertext (see last page).

2. Decrypting a Playfair Message

You should have received a sheet with a Playfair cipher grid/matrix and some encrypted ciphertext. Use the rules to determine what the original message said.

From (group name): ______________________________

To (group name): ______________________________

Encrypted message (ciphertext):

Decrypted message (plaintext):