Monoalphabetic Cipher. A monoalphabetic cipher is a substitution cipher in which the cipher alphabet is fixed through the encryption process. All of the substitution ciphers we have seen prior to this handout are monoalphabetic; these ciphers are highly susceptible to frequency analysis.

Polyalphabetic Cipher. A polyalphabetic cipher is a substitution cipher in which the cipher alphabet changes during the encryption process.

The Playfair Cipher (see page 377 in The Code Book)

i. Choose a keyword, for example \textit{KEYWORD}.

ii. Using your keyword, create a $5 \times 5$ grid is the following way.

\begin{center}
\begin{tabular}{cccc}
K & E & Y & W & O \\
R & D & A & B & C \\
F & G & H & I/J & L \\
M & N & P & Q & S \\
T & U & V & X & Z \\
\end{tabular}
\end{center}

Like a keyword substitution cipher, we write the keyword (removing repeated letters if necessary) and then write the rest of the alphabet in order, skipping letters already used for the keyword. We also combine ‘I/J’ into a single letter.

iii. To encrypt, first break the plaintext into two-character blocks.

iv. For each two-character block, one of the following occurs:

(a) The two characters are in the same row: in this case, replace the two characters by the letters to the immediate right of each (wrapping to the beginning of the row if necessary.

(b) The two characters are in the same column: in this case, replace the two characters by the letters immediately beneath each (wrapping to the top of the column if necessary.

(c) The two characters are in different rows and different columns: in this case, replace the characters by the two characters sharing a row/column relationship with the two characters; for instance in the grid above, we replace SA by PC since ACPS form the corners of a rectangle in the grid. Notice we read P first since it shares a row with S.

v. Use the encrypted character-pairs to form the ciphertext.

1. Choose a keyword of your choice and create the corresponding $5 \times 5$ grid.
2. Using your grid from the previous page, choose a plaintext message and encrypt it with the Playfair Cipher.

3. Pass the ciphertext and keyword to your partner. Use your knowledge of the encryption process to figure out the decryption process and decrypt your partner’s message.

4. What are the consequences of combining ‘I/J’ as we did?

5. Look back over your plaintext and ciphertext. Was at least one single letter used to encrypt two different letters at some point in the encryption process? Give some examples of this.

6. Do you think that the Playfair Cipher has vulnerabilities to cryptanalysis, in particular frequency analysis? Why or why not?