Playfair Cipher

What about encrypting pairs of letters?

Theory: \(26^2 = 676\) possible keys!

Unwieldy, so how can we make it easy to implement but take advantage of encrypting 2 letters at a time?

Keyword: ENGINEERS

1. Pick keyword
2. Remove duplicates
3. Put in 5x5 grid: Top left
4. Fill in rest in order

Shared Key

Plain: SALLY SELL S SEAS SHELLS

Adjusted: SA LQ LY SE LQ LS SE AS HE LQ LS

Plaintext

(Digraphs)
Rules to encrypt:

"SA"

1) Find both letters in the grid

(a) same row (SA)
(b) same col (SE)
(c) diff R+C \rightarrow form box (HE)

(a) encrypt by moving right (cyclically) one space
   
   SA \rightarrow AB

(b) encrypt by moving down (cyclically) one space
   
   SE \rightarrow FS

(c) encrypt as opposite corners of the box, each letter encrypts as a letter on the same row
   
   HE \rightarrow FN (common error flipping repeat order)

SA LR LY SE LQ LY SE LQ LS SE AS HE LQ
\downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow
AB KT TJ FS KT TJ FS KT FC FS BA FN KT

Decrypt:

(a) row \rightarrow left 1 cyclic

(b) col \rightarrow up 1 cyclic

(c) box \rightarrow SAME!
Signs of Playfair

1) even msg length (10 msg all even length...)
   hmmm...

2) Rarer consonants appear more frequently
   J,K,Q,Z,X

3) no repeated letters in digraphs

4) frequency of digraphs looks like English digraph frequencies

Attaching Playfair:

Helps if you have some matching plain/cipher text:

plain

\[ AES \]

\[ PL \quad AY \quad FA \quad IR \]
cipher

\[ QK \quad FV \quad GB \quad LE \]

Strange

ILL close
but ER NOT
in key word