

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

E	N	G	I/J	R
S	A	B	C	D
F	H	K	L	M
O	P	Q	T	U
V	W	X	Y	Z

Plain: SALLYSE~~L~~SSEASHELLS

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)

E	N	G	J	R
S	A	B	C	D
F	H	K	L	M
O	P	Q	T	U
V	W	X	Y	Z

(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 order)

SA	LQ	LY	SE	LQ	LY	SE	LQ	LS	SE	AS	HE	LQ
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
AB	KT	TJ	FS	KT	TJ	FS	KT	FC	FS	BA	FN	RT

Decrypt:

(a) row \rightarrow left 1 cyclic

(b) col \rightarrow up 1 cyclic

(c) box \rightarrow SAME!

Signs of Playfair

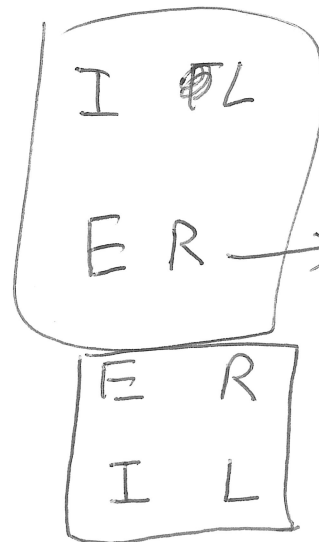
- 1) even msg length (10 msg all even length...)
hmmm...
- 2) Rare consonants appear more frequently
J, K, Q, Z, X
- 3) no repeated letters in digraphs
- 4) frequency of digraphs looks like English digraph frequencies

Attacking Playfair:

Helps if you have some matching plain/cipher text:

plain	AS	PL	AY	FA	IR
		↓	↓	↓	↓
cipher		QK	FV	GB	LE

SECRET
~~AS~~
 AB FG
 IKL
 PQ
 V Y



Strange
 ILL close
 but
 ER NOT
 in keyword

