CIS3362 9/10/2021

(1) Quizzes Still Being Graded - Returned Monday

(2) Playfair Cipher

- Old stuff monoalphabetic
- (a) Why not "group" letters at a time to encrypt? (Polyalphabetic)
- (a) Process 2 letters at a time.
- (b) Easy to do by hand!

Secret Key Word: MILLENIAL
x - - x - x

→ MILENA

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

Fill in keyword.

Take all unused letters + fill in, in alphabetic order.

MESSAGE: I WE NT TO THE ST OR E

BI NM SY YT RO LT YT TJ

Box: Use opposite corners, with letter on same row

Same Column: Replace each letter with the one below it, using wrap around

Same Row: Replace each letter w/ the letter on the right, wraparound

Identifying factors

(1) No double letters in digraph spots

(2) even length

Harder than past ciphers

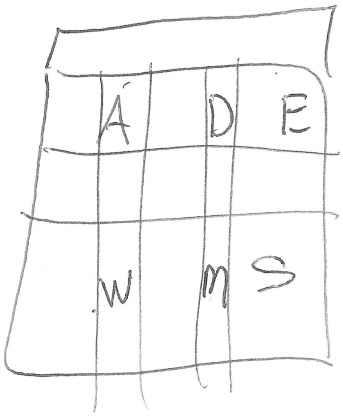
Clearly frequency info by letter is destroyed! frequency of digraphs is preserved but you need way more of this to set good patterns.

Playfair - pretty hard w/ciphertext only

Hill2 - small amount of matching plain/cipher text!

AS | AM

EW DW



D A E

M W S