CIS 3362 9/6/24

Quiz 1 - Returned Monday ✓✓ Playfair
Hmk 3 - Posted Today (give matching plain-cipher in a few days)

Polyalphabetic Ciphers
- processing multiple letters at a time

Charles Wheatstone
- easy by hand
- better/more secure than Sub, Vig

Key is just a regular word
↳ use to fill 5×5 square

"TEMPERATURE"

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

Plaintext: X
"SHEWENTTOTHESTORE"

Encrypt pairs of letters at a time. 2 letters must be different.

1. Box Case
   SH → OK
   grab opposite corners of the box, a letter encrypts to the letter on same row of the box but opposite side

2. Same Col Case
   EW → UE
   encrypt with the letter directly below, wrapping around to the top of same column if necessary.

Cipher	OK	UE	UW	MV	ML	MF	RN	ML	TM
Plain	SH	EW	EN	TX	TO	TH	ES	TO	RE

If last letter is by itself add padding character.

3. Same Row

RE → TM

encrypt with the letter directly to the right, wrapping around to the left end of the same row, if necessary

Decrypt

1. Box (same process, grab opposite corners, stay on same row) OK → SH
2. Col (move up 1 row on the same col, wrap around if necessary)
3. Row (move left 1 col on the same row, wrap around if necessary.

Identifying Playfair

1) even # chars
2) Rare consonants J, K, Q, X, Z appear frequently
3) When divided into pairs, no double letters.
4) Frequency of the digrams approximates that of English.
5) No letter ever encrypts to itself
6) To reversed letters in ciphertext are the same pair reversed in plaintext

CK and KC → stand for the same 2 letters in reverse order.

7) each plaintext letter can only be encrypted as one of 5 ciphertext letters.