

CIS 3362

High-level ORG

W1, W2 - Monoalphabetic Ciphers

Extended Euclidean Algorithm
(GCD, Modular Inverse)

W3, W4, W5 - Polyalphabetic Ciphers (Vigenere is one)
Anything Pre-Computer

EXAM #1

1800s - Vigenere Broken

Code Makers - let's try new ideas

Polyalphabetic - "poly = more than 1" alphabet

Playfair

Lord Playfair, Charles Wheatstone

Beale Ciphers (hidden treasure)

Natural Leap - ~~P~~ Substitute Pairs!

keyword: MOONSTONE

Encrypt Row

Move Right

Cyclically 1

spot

Encrypt Col

Move Down

Cyclically 1 spot

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

5x5 GRID

Encrypt Rectangle

X	W
Z	Y

$XY \rightarrow WZ$

$WZ \rightarrow XY$

Use letters in opposite corners, matching row

Plaintext: SALLYWENTTOTHESHORETU

SA LX LY WE NT TO TH

Ciphertext: OC QV RV VA SM MN NK

Note: For double letters pad with X (I'll give you padding char in general.)

ES HO RE TU

CM GN LC DZ

Decrypt

Box - Opposite corners matching rows
(call the encrypt function)

Row - Move left 1 spot cyclically

Col - Move up 1 spot cyclically

Code storage

location['M' - 'A'] = 0

location['O' - 'A'] = 1

location['E' - 'A'] = 5 // row 1 col 0