CIS 3362 9/21/22

Transposition

Typed

1) Key a number
2) Railfence
3) Triangular
* 4) Permutation
* 5) Column Perm
6) Double Trans

Permutation (Spillman book)

Key = [3, 6, 2, 1, 5, 4]

key[i] is location of ith char block

PLAIN: TODAY IS WEDNES DAYXX

CIPHER: ADTIYO DESENW YASXXD

To break - guess block size

A D T I Y O
D E S E N W
Y A S X X D

goal rearrange columns until you see words

Column Permutation

(8)(6)(2)(7)(3)(4)(5)(1)

Keyword: UMBRELLA

assign a perm based word

⇒ sort letters in alpha order + label them numerically this way

ties → left to right

write plain row by row

8	6	2	7	3	4	5	1
W	E	A	L	R	E	A	D
Y	C	O	V	E	R	E	D
T	H	I	S	I	D	E	A
W	H	E	N	W	E	S	A
W	A	D	F	G	V	X	

Cipher: DDAAAOIEDREIWG ERDEV AEESX ECHHA LVSNF WYTWW

How to decrypt w/ key: $\lceil 39/8 \rceil = 5$ long col length

chars = 39 [$39 \% 8 = 7 \Rightarrow$ 1 short column]

last column

compute this col w/ have 4 letters. I need the 1st 4 letters but write them down column

8	6	2	7	3	4	5	1
W	E	A	L	R	E	A	D
Y	C	O	V	E	R	E	D
T	H	I	S	I	D	E	A
W	H	E	N	W	E	S	A
W	A	D	F	G	V	X	

QUIZ TOPICS

0) Playfair
1) ADFGVX AID: calculator

2) Hill Cipher
   - encrypt
   - get decryption key given encryption
   - Setting up equations for matching plain/cipher attack

3) Enigma
   - counting # rotor settings
   - ?

4) Navajo
   - ?

5) Transposition
   - Column Perm
   - Perm
   - What index a character will end up in.

   ] encrypt or decrypt w/ key

Code Notes

write msg in grid reg way

p[0] p[1] ... p[k-1]
p[k] p[k+1] ... p[2k-1]

find column 0 then column 1

we stored 7, 5, 1, 6, 2, 3, 4, 0

0 → 7
1 → 2 etc.
2 → 4