CIS 3362 9/8/2025

Polyalphabetic Ciphers - might process more than 1 letter at a time.

Era 1800s - WW II (pre computer but more complicated than substituting for each letter)

~~TRAS~~

TRANSPOSITION

↳ Reordering items in a message.

Write ~~Read~~ letters in rows but read out in columns left to right

PERMUTATION CIPHER

block size 8 , [3,6,1,8,2,7,4,5]

PLAIN: TODAYIS SEPTEMBER EIGHTHXX

DITSOSAY TBERPEEM GHEXIXHT

Note: Also looked @ typed notes for Railfence + Transver Transposition

COLUMN PERMUTATION

5 7 3 1 4 2 6

Keyword: ORLANDO

5	7	3	1	4	2	6
T	H	I	S	C	L	A
S	S	I	S	A	L	W
A	Y	S	N	E	A	R
L	U	N	C	H	T	I
M	E	S	O	I	A	M
A	L	W	A	Y	S	H
U	N	G	R	Y	W	H
E	N	I	T	E	A	C
H	H	E	R	E		

label from keyword read the columns down in order by the number labels

61 letters

61 ÷ 7 = 5

5 cols 9 letter

2 cols 8 letter (col labels 2, 6)

OUTPUT: SSNCOARTR LLATASWA

IISNSWGIE CAEHIYYEE

TSALMAUEH AWRIMHHC

HSYUELNNH

Double Transposition & twice!!! ← DO this

Most Modern Crypto uses both of these techniques

Diffusion ↑ REORDERING and Confusion ↑ SUBSTITUTION