

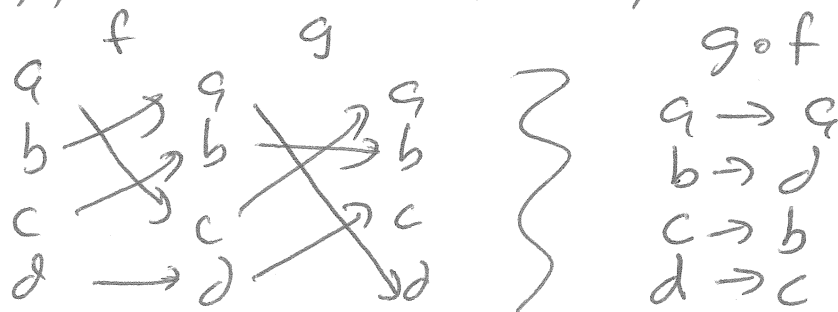
- ① Compound Ciphers
- ② Transposition
- ③ ADFGVX (German Cipher during WWI)

→ function composition

$$f_{k_1}(x) = c_1 \rightarrow g_{k_2}(c_1) = c_2$$

$f \rightarrow$ substitution, $g \rightarrow$ substitution

$g(f(x)) \rightarrow$ is this any more secure?



$$f(x) = ax + b$$

$$g(x) = cx + d$$

$$g(f(x)) = c(ax + b) + d \pmod{m}$$

$$= \cancel{ax}cx + (bc + d) \pmod{m}$$

(transposition (switching rows and cols))

Column transposition

Keyword: A L P H A

Message:

A	L	P	H	A
1	4	5	3	2
H	E	L	L	O
W	E	L	C	O
M	E	B	A	C
K	A	F	T	E
R	T	H	E	W
E	E	K	E	N
D				

Step 1 - sort letters
in order write numbers
underneath, break ties left
to right.

Step 2: Write message
in grid top going
down, left to right.

Step 3: read the columns
in number order

HWMKREDOOCEWNLCAEEEEEEATE

LLBFHK

Doesn't change any letters but it moves
them around [DIFFUSION]

Changing characters [CONFUSION]

Claude Shannon - "confusion + diffusion"

NOTE - be able to decrypt transposition
given the key! (Pay attention to int div
mod in computing column
lengths.)

ADFGVX

Before 1918, this was ADFGX. V was added during the war.

Radio Morse Code - Morse Codes for A, D, F, G, V, X and significantly different + less likely to be confused for a different letter in the set.

Key 1 for Part 1 is "similar" to Playfair

	A	D	F	G	V	X
A	zero	O	H	9	T	A
D	E	C	W	Z	V	5 (five)
F	R	8	4	G	two	is I
G	K	J	U	X	P	Y
V	6	S	B	N	D	Q
X	F	3	M	one	7	L

Message ITSMONDAYMORNING

* FX AV VD XF AD VG VV AX GX XF AD FAVG FX VG FG

for each symbol, find it, encrypt as row label followed by column label

Key 2: keyword for column transposition

Key2: K N I G H T S

K	N	I	G	H	T	S
4	5	3	1	2	7	6
F	X	A	V	V	D	X
F	A	D	V	G	V	V
A	X	G	X	X	F	A
D	F	A	V	G	F	X
V	G	F	G			

Cipher: VVXVG VGXG ADGAF FFADV
XAXFG XVAX DVFF

Code

key word was

0	1	2	3	4	5	6
P	R	I	V	A	C	Y

(4), 5, 2, 0, 1, 3, 6

perm[0] = 4

means the column to
read first(0) is in
position 4