# CIS3362 9/22/2021

1. Double Transposition
2. Quiz Review + Rules

→ Use 2 keywords

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

a) KNIGHTS 3, 4, 2, 0, 1, 6, 5

b) MOONSHINE 3, 6, 7, 4, 8, 1, 2, 5, 0

(3)(6)(7)(4)(8)(1)(2)(5)(0)

3 4 2 0 1 6 5
K N I G H T S

T H I S I S A
S H O R T M E
S S A G E

Read Cols → SRGITEIOATSSHHSAESM

3 6 7 4 8 1 2 5 0
M O O N S H I N E

~~S R G I T E O A T~~
~~S S H H S A E S M~~

3 6 7 4 8 1 2 5 0
S R G I T E I O A
T S S H H S A E S
M

Read Cols → ~~TMEAOESSIHASRSGHTS~~

Read Cols → ASESIASTMIHOERSGSTH

If I apply 2 affine cipher is it more secure than 1 affine cipher?

Is it $312 \times 312$ possible keys?

$f_1(x) = (ax+b) \bmod n$
$f_2(x) = (cx+d) \bmod n$

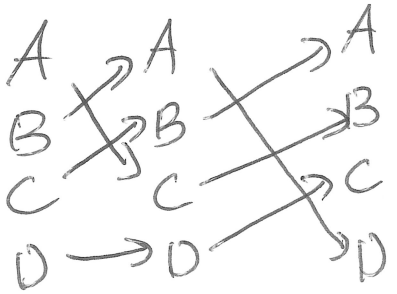
$\gcd(a,n)=1$
$\gcd(c,n)=1$

$$f_2(f_1(x)) = f_2(ax+b)$$
$$= c(ax+b)+d \pmod n$$
$$= acx + bc + d \pmod n$$

$\gcd(ac,n)=1$

2 SUBS?

Confusion + diffusion




equiv

$A \to B$
$B \to D$
$C \to A$
$D \to C$

But for transposition, 2 applications yields a "greater key space" and is harder to break.

Most Symmetric (you + I share a secret key) ciphers do LOTS of substitution AND transposition in multiple phases (rounds).

# QUIZ 2

(1) 50 minutes
(2) No formula sheet
(3) Calculator

TOPICS: Playfair, Hill, ADFGVX, Enigma, Navajo, Transposition / Column Perm