(1) Double Transposition
(2) Quiz Review + Rules

9 Use 2 keywords
   a) KNIGHTS
   b) MOONSHINE

   3 4 2 0 1 6 5

KNIGHTS

THIS IS A
SHORTME
SSAGE

Read Cols → SRGITEIOATSSSHHSAESM

3 6 7 4 8 1 2 5 0

MOONSHINE

SRGITEIOAT
SSSHHSAESM

Read Cols → TMEAOESSSTHASRSGHTS

Read Cols → ASESIASTMIHOERSGSTH
If I apply 2 affine cipher is it more secure than 1 affine cipher?

Is it $312 \times 312$ possible keys?

$$f_1(x) = (ax + b) \mod n \quad \text{gcd}(a, n) = 1$$
$$f_2(x) = (cx + d) \mod n \quad \text{gcd}(c, n) = 1$$

$$f_2(f_1(x)) = f_2(ax + b)$$
$$= c(ax + b) + d \quad (\mod n)$$
$$= acx + bc + d \quad (\mod n)$$
$$\text{gcd}(ac, n) = 1$$

2 Subs?

Confusion + diffusion

\[\begin{array}{cccc}
B & B & B & B \\
C & C & C & C \\
D & D & D & D \\
\end{array}\]

equiv

\[\begin{array}{cccc}
A & B & B & D \\
B & C & A & C \\
C & D & D & C \\
D & D & D & D \\
\end{array}\]

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, ADFGXVX, Enigma, Navajo, Transposition/Column Perm