

9/13/19 ①  
16

ADFGVX

|   | A | D | F | G | V | X |
|---|---|---|---|---|---|---|
| A | N | ④ | 1 | C | 3 | H |
| D | 8 | ① | B | 2 | O | M |
| F | E | S | W | R | P | D |
| G | 4 | F | 6 | ⑧ | ⑦ | I |
| V | 9 | J | 0 | K | L | Q |
| X | S | U | V | X | Y | Z |

$$36 = 26 + 10$$

↓      ↓  
letters    digits

randomly fill square  
with all 36 chars.

ATTACK AT 1200AM

Step 1: do substitution by  
chart.

A D D D D A G V G A D D D A F D G V F V F A D D X  
 a t t 1 2 0 0 a m

Step 2: Keyword (PRIVACY)

④ ⑤ ③ ⑥ ① ② ⑦

P R I V A C Y

A D D D D D A

D A G V G A D

D D A F D G V

F V F A D D X

③ ⑥ ⑦ ⑧ ② ① ④ ⑤  
F O O T B A L L

Transposition

Read in the order of the #s of the columns:

D G D D D A G D D G A F ~~A D D~~ A D D F D A D V D V F A A D V X  
 1      2      3      4      5      6      7

→ Ciphertext

$msglen = 30 / 7 = 4$  (all cols 4 or 5)  
 $30 \% 7 = 2$  (# cols that are 5)

9/13/19 ②

THIS IS A SHORT MESSAGE

②③④⑤

CHAIR

THIS IS  
A SHORT  
MESSAGE

ISMGTSRSHATASHEEIOS

ISMGTSRSHATASHEEIOS

THIS IS  
A SHORT  
MESSAGE

THIS IS  
A SHORT  
MESSAGE

Keep Take Home MSGs

① Combination of 2 different ciphers into one can make a stronger cipher than either system.

Claude Shannon  
"confusion" + diffusion  
Substitution  
the effect of a single plaintext letter ~~goes to~~ spreads to multiple places in the ciphertext

# Composing Ciphers

① substitution followed substitution?

$$A \rightarrow Q \rightarrow B \iff A \rightarrow B$$

② affine followed by affine?

produces another valid affine  
(no better)

③ Vigenere followed by vigenere?

|   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|
| A | G | E | A | G | E | A | G | E | A | G | E |
| F | R | U | I | T | F | R | U | I | T | F | R |

effect is on a vigenere with  
keyword length  $\text{lcm}(a,b)$ , where  $a, b$   
are the lengths of the 2 keywords.

order of adding does not matter