CIS 3362 9/12/22

German WWI Cipher

ADFGVX

↳ only letters in ciphertext

reason: Morse code symbols "very different" according to Wikipedia!

Notes: Showed grid from typed notes!

6x6 ~~grid~~ grid

Row/col labels are A, D, F, G, V, X

contents: 26 letters, 10 digits randomly placed.

To encrypt a letter/digit, find its row + col in grid. Ciphertext is row label, col label.

Mathematically this is exactly substitution on 36 symbols. Input = P

Call this intermediate output C_1

~~Senco~~ Second key is a keyword.

Let's choose KNIGHTS!

(1) Copy key word into columns.

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

(2) Copy C_1 into grid row by row going left to right in each row. Rows top → bottom.

(3) Sort keyword letters in alpha order label this order numerically. For repeated letters, go left to right

(4) Read ciphertext down columns in numeric order.

Ciphertext: XGAVF XXVV ADFXD FVADA XFXXD

FAAV FDDA

Why better than what we've seen previously?

Claude Shannon - father of information theory

Confusion - substitution (changing symbols)

diffusion - something stirring one place affecting other places (a plaintext char affecting ciphertext character(s) in different locations)

Decrypt - REVERSE the steps

to encrypt $g(f(x, k_1), k_2)$

to decrypt $f^{-1}(g^{-1}(C, k_2), k_1)$