CIS 3362 8/29/22

So far: Shift, Affine $f(x) = 3x + 2$

X	f(x)
A	D
B	E
C	F
⋮	⋮

X	f(x)
A	C
B	F
⋮	⋮

X	A
Y	B
Z	C

Z	Z (fixed point)

Generalize this idea → any valid chart could be a key!

X	f(x)	
A	P	26
B	A	25
C	M	24
D	X	etc.

(1) Pros
- lots of possible keys!!!
  $26! \sim 10^{18}$ or more

(2) Con
harder to store key (bigger)

But, since about the year 1000, substitution ciphers have been decrypted!

HOW?

al-Kindi - different letters appear diff # of times
substitution - set of letter freq. stays the same!

invariant in substitution cipher ⟹ LETTER FREQ!

⟹ GUESSING, PROCESS OF ELIMINATION
⟹ OTHER LANG FEATURES

frequencies won't be a perfect map!

in English 12.7% → E
9.1% → T

In small samples "error bar" is large.
Some samples might be biased.

Usually most freq letter is either E, T, A, O, S, H, R

Common digraphs, trigraphs "ED", "ING", "AND", "EN"

(1) Make guesses, but
(2) Be willing to backtrack if you hit something impossible.
(3) KEEP TRACK OF WHAT YOU'VE TRIED!

Beginning rough! 2hrs → 6 letters
next 20 letters takes 10 min!

Queen Mary Communication

1) Hide in beer barels (steganography)

2) Code
Substitution +
(1) 36 code words (the, for, it, etc.)
(2) 4 null characters
(3) doubleth – next char doubled "rr"
"doubleth" [code r]

3) Loyalists bribed a guard!
– guard double paid by Queen!

4) Sir Francis Walsingham (Queen Eliz. cryptanalyst)
also getting messages!

Additional bells & whistles

delete char
100 cipher text (00 ... 99)
assign by let freq e → 12 diff codes
t → 9 code
a → 8 codes
each 100 codes
will appear roughly equally!

MOST OF THESE WERE EVENTUALLY BROKEN!