CIS 3362 8/30/21

(1) Please wear your mask!

(2) Substitution Cipher

Plain		Cipher
A	→	X
B	→	C
C	→	Q
D	→	P
E	→	A
⋮		⋮

permutation of (A, B, C, ... Z)

"XCQPA..." is encryption key

$26 \times 25 \times 24 \times \cdots \times 1 = 26!$

~ big ~~very bigger~~ 10^{12}

4×10^{26}

Point: Brute Force Infeasible (by hand or computer!)

What makes cipher text not random?

(1) Letter Frequency
(2) Common Digrams, Trigrams
(3) Consonant/Vowel Patterns

Put this together and guess!

(1) Carefully document your guesses.
- so you don't retry stuff

(2) If stuck, see if you can undo an assumption.

(3) See if you can guess a word.

Elementary Cryptanalysis - Sinkov

HISTORY

Code Book - Simon Singh

Queen Mary of Scots
20 code symbols for common words
null characters

Substitution first broken ~970 AD
Al-Kindi

Queen Elizabeth's Cryptographer:
Sir Francis Walsingham