

CIS 3362 - 8/28/23

learned: shift 26 poss keys } too few...
affine 312 poss keys } someone can try them all

flat assumption

A → C

B → X

C → P

D → Q

Why not allow a full chart w/ 26 rows?

How many possible keys?

A → 26

B → 25

C → 24
⋮

$26 \times 25 \times 24 \times \dots \times 1$

$= 26! \rightarrow \text{big \#}$

Z → 1

Substitution cipher

Generalization of our flat assumption that each letter gets substituted by another

Cryptanalysis - using information to narrow down the search for the key so you don't have to try them all.

Substitution Cryptanalysis

① In encryption/decryption the set of letter frequencies is unchanged. (invariant)

- Useful because different letters appear a different % in plaintext.

② Repeated digrams/trigrams/n-grams

published
in btw
900-1000

Al-Kindi.

③ Elementary Cryptanalysis - Sinkov

- Consonant-Vowel Patterns

- Pattern XX

Queen Mary Code (1500s)

20 code words substituted by symbols. (30+)

null characters 4

backspace char 1

$26 + 5 + 35 \sim 60-70$
total symbols

hid fact communicating by putting mss in beer barrels

Queen Elizabeth's Cryptographer: Sir Francis Walsingham

* Theme: human behavior plays a huge role
in codes that get broken throughout
history.