

CIS 3362 8/31/26

Substitution Cipher

Plain	Cipher
-------	--------

A	Q
---	---

B	Z
---	---

C	M
---	---

D	E
---	---

⋮	
---	--

Z	P
---	---

26! possible

lists (too many

options to brute

force!)

Al-Kindi (late 900s)

letter frequency is invariant
under substitution

(1) Find most frequent letters

(2) Look for common words
and profile their frequency lists

THE (9%, 2%, 12%), AND (8%, 6%, 3%)

MAKE INTELLIGENT GUESSES

TRIAL ERROR + LOOK FOR PLAINTEXT
WORDS TO APPEAR.

(3) Use as many properties of target
language (double letters, vowel patterns, etc.)

Beginning part very slow with lots of wrong turns. After you match 1st 5 letters or so it's like wheel of fortune; it goes fast.

Queen Mary of Scots

Scotland - Mary (Catholic)

English Queen: Queen Elizabeth I (Protestant)

~1570 Elizabeth imprisons Mary

Gilbert Gifford - volunteers to sneak messages to Mary in jail. Hidden in beer barrels (Stegsnography), letter encrypted.

20 code words - substitute a symbol for a whole word (words are common ones)

blank characters

backspace character

Gifford - DID DOUBLE DUTY

→ PAID BY MARY

→ PAID BY ELIZABETH TO

GIVES CIPHERTEXT TO
FRANCIS WALSINGHAM, ELIZABETH'S
COURT CRYPTOGRAPHER

VIGENERE

Created in 1500s to thwart frequency analysis. Remained unbroken until the 1800s!

10, 13, 8, 6, 7, 19, 18
keyword: KNIGHTS

Plain: THIG(S)THESECONDWEEKOFCLASS

19, 7, 8, 18, 8, 18, 19, 7, 4, 18, 4
+ 10 13 8 6 7 19 18 10 13 8 6

29, 20, 16, 24, 15, 37, 37, 17, 17, 26, 10

3 20 16 24 15 11, 11, 17, 17, 0 10
D V Q Y P L L (R R) A K
= =

Two of the same plaintext char can map to different ciphertext chars.

Two of the same ciphertext char can map back to different plaintext letters.

PARADIGM SHIFT

JUST PLAIN MESSES UP
LETTER FREQUENCY