CIS 3362 8/29/25

1) Schedule → M - Labor Day
W - QUIZ
closed notes
formula sheet
11[15] → skip 11[25]
extend 12[25]
F - Do not come to class
Watch Playfair Video

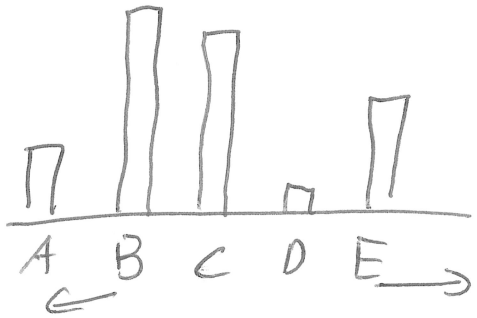
2) Breaking Vigenere + MIC
↓
Kasiski Test
1. of C.
↳ Find key word length

Ciphertext $c_0\ c_1\ c_2 \cdots c_{n-1}$ length n
keyword length k

BINS 0 $c_0, c_k, c_{2k}, c_{3k} \cdots$ ~~$c_{(\frac{n}{k}-1)k}$~~ $n-k$
BIN 1 $c_1, c_{k+1}, c_{2k+1} \cdots$ c_{n-k+1}
⋮
BIN $k-1$ $c_{k-1}, c_{2k-1} \cdots$ c_{n-1}

all letters in bin 0 shifted by g_0
" " " " 1 shifted by g_1, etc.

LETTERS A B C D E



Imagine bar graph conveyor belt (circular)

bin 0 
move left
1 slot A B C D E

So if k_0 = 'B' then this would be plaintext letters.

VISUALLY → try each cyclic shift of a bin and find the one that looks like English frequencies

How can we do this mathematically w/o drawing lots of graphs and eyeballing them?

Mutual Index of Coincidence

Problem: Get 1 candy from each of 2 neighbors. What is the probability they are same?

	N1	N2
Snickers	10	~~80~~ 30
Twix	20	5
Skittles	30	5
Mars	40	10

$$\frac{10\times30+20\times5+30\times5+40\times10}{100\times50}$$

$$= \frac{300+100+150+400}{5000}$$

$$= \frac{950}{5000} = \frac{95}{1000} = \boxed{\frac{19}{200}}$$

$$MIC(S_1, S_2) = \frac{\sum_{i=1}^{k} f_i \times g_i}{n \times m}$$

$n = \sum_{i=1}^{k} f_i$ $\quad f_i$ is # of item i in S_1

$m = \sum_{i=1}^{k} g_i$ $\quad g_i$ is # of item i in S_2

If your bin is real English this tends to maximize MIC calculation

Original bin 0: 10, 50, 45, 5, 20

bin 1: 8, 25, 15, 40, 45

Martin Language: .2, .1, .3, .3, .04

$$\left(\begin{matrix} 10 + 50 + 45 + 5 + 20 \\ \times .22 \times .1 \quad .3 \times .34 \times .04 \end{matrix}\right) / 130$$

$$= \frac{23.2}{130} = .178$$

Shift 1: 50 45 5 20 10 (.22 .1 .3 .34 .04) $= \frac{24.2}{130} = .186$

Shift 2: 45 5 20 10 50 (.22 .1 .3 .34 .04) $= \frac{21.8}{130} = .168$

Shift 3: 5 20 10 50 45 (.22 .1 .3 .34 .04) $= \frac{24.9}{130} = .192$

Shift 4: 20 10 50 45 5 (.22 .1 .3 .34 .04) $= \frac{32.16}{130} = .247$