

CIS 3362 8/27/2025

1) Schedule

2) Vigenere Cipher

↑

→ 8/27 Today

8/29 Breaching Vigenere IC, MIC

9/1 LABOR DAY

9/3 QUIZ #1

9/5 ~~DO~~ DO NOT COME TO CLASS!
INSTEAD WATCH PRE-POSTED
PLAYFAIR VIDEO

→ ISOOS (Very Simple)

PLAIN TEXT : U C F K N I G H T S
20, 2, 5, 10, 13, 8, 6, 7, 19, 18

KEY: HOUSE +7 14 20 18 4 7 14 20 18 4
7, 14, 20, 18, 4

Unbroken
ISOOS →

early
1800s

27	16	25	28	17	15	20	27	37	22
↓			↓				↓	↓	↓
1	16	25	2	17	15	20	1	11	22
B	Q	Z	C	R	P	U	B	L	W

How to Break?

Helpful to know the keyword length!

(1) Kasiski Test

(2) Index of Coincidence Test

→ Imagine line up 2 copies of same trigram or longer

MORNING
HOUSE

76

BXP

MORNING
HOUSE

~~188~~

BXP

→ (length of keyword) | (~~188~~ - 76)

112

different repeat 240 difference

d | 112

1

d | 240

$$240 = 2 \times 112 + 16$$

$$112 = 7 \times 16$$

$$\begin{array}{r} 16 \\ 7 \end{array}$$

Index of Coincidence Test

Define $IC(S)$, where S is a multi-set of objects (letters) as the probability that 2 randomly selected items from the set are the same.

10 Twix, 20 Snickers, 5 Mars, 15 Skittles

$$\frac{10}{50} \times \frac{9}{49} + \frac{20}{50} \times \frac{19}{49} + \frac{5}{50} \times \frac{4}{49} + \frac{15}{50} \times \frac{14}{49}$$

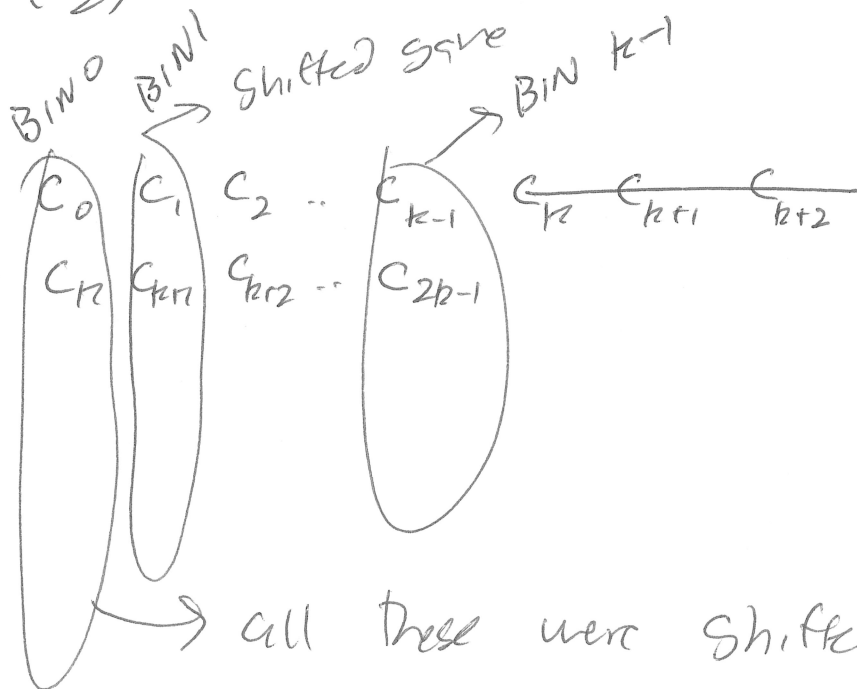
$$= \frac{90 + 380 + 20 + 210}{50 \times 49} = \frac{470 + 230}{50 \times 49} = \frac{700}{50 \times 49} = \frac{14}{49} = \boxed{\frac{2}{7}}$$

$$\frac{\binom{10}{2} + \binom{20}{2} + \binom{5}{2} + \binom{15}{2}}{\binom{50}{2}} = \frac{2}{7}$$

$$\sum_{i=1}^k \frac{f_i \times (f_i - 1)}{n \times (n - 1)}$$

$f_i = \# \text{ of letters } i$

$$\sum_{i=1}^k f_i = n$$



$$IC(\text{rand eng}) = \frac{1}{26}$$

letter
not from
words

0.03846

$$IC(\text{letter reel text}) \approx 0.067$$

12.7% Twix, 8.2% Snickers, 9.1% Skittles etc
0.1% dots

Try each keyword length

for (int k=3; ; k++) {

// Break ciphertext into k bins

// Calculate IC of each bin

k=3 .043 .051 .037 X

k=4 .039 .052 .051 .048 X

k:

:

k=7 .078 .081 .059 .069 .088 .065
 .077

Wait until almost all the IC values
are close to or above .067.