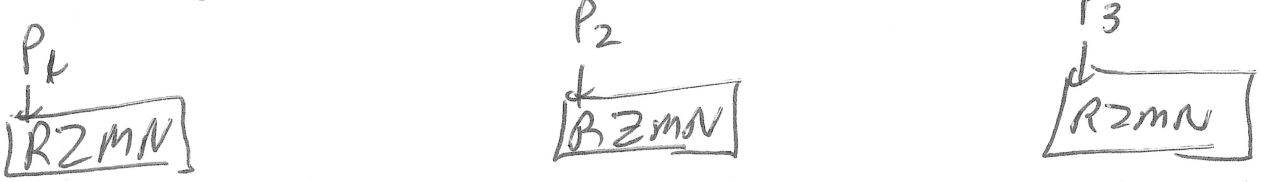
CIS 3362 8/30/24

1. Breaking Vigenere
   - Kasiski Test
   - Index of Coincidence
   - Mutual Index of Coincidence
2. Cryptool
3. Quiz Wed



repeated n-grams ciphertext

length keyword = gcd ($P_2 - P_1$, $P_3 - P_2$, $P_5 - P_4$)

QZRBS QZRBS

↑ P_5

P_4

Index of Coincidence is defined on a multi set of objects

10 Twix
8 Snickers
22 Skittles
25 Mars

randomly select 2 items out of the whole. What is probability they are the same type?

$f_1, f_2, \ldots f_k \qquad f_1+f_2+f_3+\ldots+f_k = n$

$10, + 8, + 22, + 25 = 65 \ (n$

$$\frac{10}{65}\times\frac{9}{64} + \frac{8\times7}{65\times64} + \frac{22\times21}{65\times64} + \frac{25\times24}{65\times64}$$

1st twix

$$= \frac{90+56+462+600}{65\times64}$$

$$= \frac{1208}{65\times64} = \frac{302}{65\times16} = \frac{151}{65\times8} = \boxed{\frac{151}{520}}$$

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

We use this with frequency of letters

Cipher : $c_0, c_1, c_2, \ldots$

Guess keyword length is 5

Shifted k_0 bin 0 : c_0, c_5, c_{10}, c_{15} frequencies should be ~~the~~ plaintext freq.

Shifted k_1 bin 1 : $c_1, c_6, c_{11}, c_{16}, \ldots$

Shifted k_2 bin 2 : $c_2, c_7, c_{12}, c_{17}, \ldots$

Shifted k_3 bin 3 : $c_3, c_8, c_{13}, c_{18}, \ldots$

Shifted k_4 bin 4 : $c_4, c_9, c_{14}, c_{19}, \ldots$

If a distribution is equally random $\frac{1}{26}$ letters is A, B, etc.

$$IC(\text{set}) \cong \frac{1}{26} = .0378 \text{ ish}$$

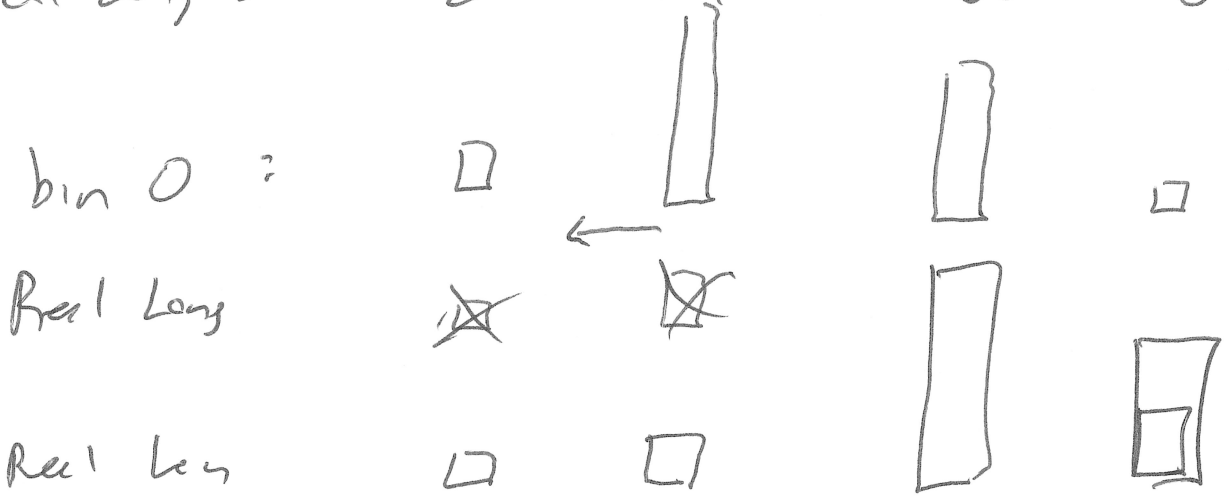
$$IC(\text{English}) \cong .0676$$

the more "off balanced" a distribution is the higher the Index of Coincidence!

If we guessed correctly, the IC of ALL the bins should be "high" near 0.07. If we guessed wrong, some bins will be lower.

Once we know the length of the keyword, what do we do?

Cipher	A	B	C	D
Bin 0:	3	18	10	1
Real Long:	20/0	40/0	60%	34%



Left Shift 0	3	18	10	1
Left Shift 1	18	10	1	3
Left Shift 2	10	1	3	18
Left Shift 3	1	3	18	10

Intuitively, try all left shifts (decrypt) on a bin, and pick the one that makes the adjusted bar graph look most like the English bargraph ↓

	3	18	10	1	set 1
b.g.1	x	x	x	x	
b.g.2	2	4	60	34	set 2

What's the probability if I grab 1 item from set 1 and 1 item from set 2, that they are the same?

Mutual Index of Coincidence : $\frac{3}{32} \times \frac{2}{100} + \frac{18}{32} \times \frac{4}{100} + \frac{10}{32} \times \frac{60}{100} + \frac{1}{32} \times \frac{34}{100}$

$f_1 + f_2 + \dots f_k = n$

$g_1 + g_2 + \dots g_k = m$

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

3, 18, 10, 1

× 2 4 60 34

LS 0 $6 + 72 + 600 + 34$

LS 1 18, 10, 1, 3

2 4 60 34

$36 + 40 + 60 + 102$

34
18
272
34

LS2 10, 1, 3, 18

2 4 60 34

$20 + 4 + 180 + 612$

LS3 1, 3, 18, 10

2, 4, 60, 34

$2 + 12 + 1080 + 340$