

9/11/19 ①

Vigenere

	P_0	P_1	P_2	P_3	...	P_{m-1}	P_m	...	P_{2m-1}	P_{2m}
+	K_0	K_1	K_2	K_3	...	K_{m-1}	K_0	K_1	K_{m-1}	K_0
	C_0	C_1	C_2	...						

Letters $C_0, C_m, C_{2m}, C_{3m}, \dots$ should have frequencies of English text

Same for $C_1, C_{m+1}, C_{2m+1}, \dots$

$C_2, C_{m+2}, \dots$

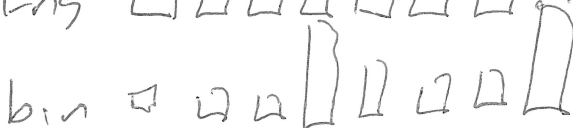
$C_{m-1}, C_{2m-1}, C_{3m-1}, \dots$

Once we know the keyword size,
what do we do?

	A	B	...	Z
bin ₀	16	3	...	
bin ₁	2	0	...	
...				
bin _{m-1}	1	1	8	...

cyclic rotation of frequencies in English

Eng 

bin 

Method #1

For each bin,

Try all 26 shift values

Calculate MIC btw english

+ this bin

Keyword letter - probably one max MIC

Mutual Index of Coincidence (A, B):
prob that a randomly chosen item from set A equals a randomly chosen item from set B.

9/11/19 ②

$$A: f_0 f_1 f_2 \dots f_{m-1} \quad \sum_{i=0}^{m-1} f_i = n_1$$

$$B: g_0 g_1 g_2 \dots g_{m-1} \quad \sum_{i=0}^{m-1} g_i = n_2$$

$$MIC(A, B) = \frac{\sum_{i=0}^{m-1} f_i g_i}{n_1 \cdot n_2}$$

10As	5Bs	3Cs	12Ds	30 ✓
2As	13Bs	9Cs	6Ds	30 ✓

$$MIC = \frac{10 \times 2 + 5 \times 13 + 3 \times 9 + 12 \times 6}{30 \times 30}$$

Method # 2

Keep bin_0 fixed (don't shift)

for bins $i=1$ to $m-1$,

try all 26 shifts

Calc $MIC(bin_0, bin_i)$

Note which shift created the max MIC

k_0 bin_0 □□□□...

$k_1 = k_0 + 9$ bin_1 □□□□... shifted back 9

$k_2 = k_0 - 3$ relative shift

$k_3 = k_0 + 17$..

try all
26 values
for k_0