Affine Cipher - Cryptanalysis

$e_{7,4}(x) = (7x+4) \bmod 26$

$e_{7,4}(4) = (7\times4+4)$
$= 32 \bmod 26$
$= \boxed{6}$ 'G'

$e_{7,4}(19) = (7\times19+4) \bmod 26$
$= 133+4 \bmod 26$
$= 137 \bmod 26$
$= \boxed{7}$ 'H'

Cipher	Plain
G →	E
H →	T

} 2 guesses based on freq.

$d(x) = (ax+b) \bmod 26$

$d(6) = 6a+b = 4 \bmod 26$
$d(7) = 7a+b = 19 \bmod 26$

$a = 15 \bmod 26$

coeff could be here

$d(6) = 6(15)+b = 4 \bmod 26$
$90+b = 4 \bmod 26$
$b = -86 \bmod 26$
$b = \boxed{18}$

mult by modular inverse

Possible Situation

$$8a \equiv 14 \mod 26$$

Note: $8^{-1} \mod 26$ doesn't exist!

$$8a = 14 + 26c, \quad c \in \mathbb{Z}$$

$$4a = 7 + 13c$$

$$\Rightarrow \boxed{4a \equiv 7 \mod 13}$$

If we got, $8a \equiv 15 \mod 26$, this equation has NO solns $\Rightarrow$ YOUR GUESS WAS WRONG!

Cryptanalysis - analyzing structure + contents of ciphertext to make deductions about the possible keys to reduce the search space.

Substitution Cipher

Plain	Cipher
A	Q
B	R
C	A
D	Z
E	F
F	B
⋮	⋮

$26 \times 25 \times 24 \times \dots \times 1$

$= \boxed{26!}$ factorial

$\prod_{i=1}^{26} i$ – plug in each integer from $i=1$ to 26, into the expression + multiply each of these terms together.

$\prod_{i=3}^{7} (2i+3) = 9 \times 11 \times 13 \times 15 \times 17$

26! is very big! $10^{20 \text{ something}} \sim 10^{26}$

Brute Force is NOT possible!!!

In 10th century an Arabic mathemician/scholar (Al Kindi) figured out that frequency information, as well as letter structure IS unchanged in ciphertexts, for substitution.

Common digraphs
Common trigraphs

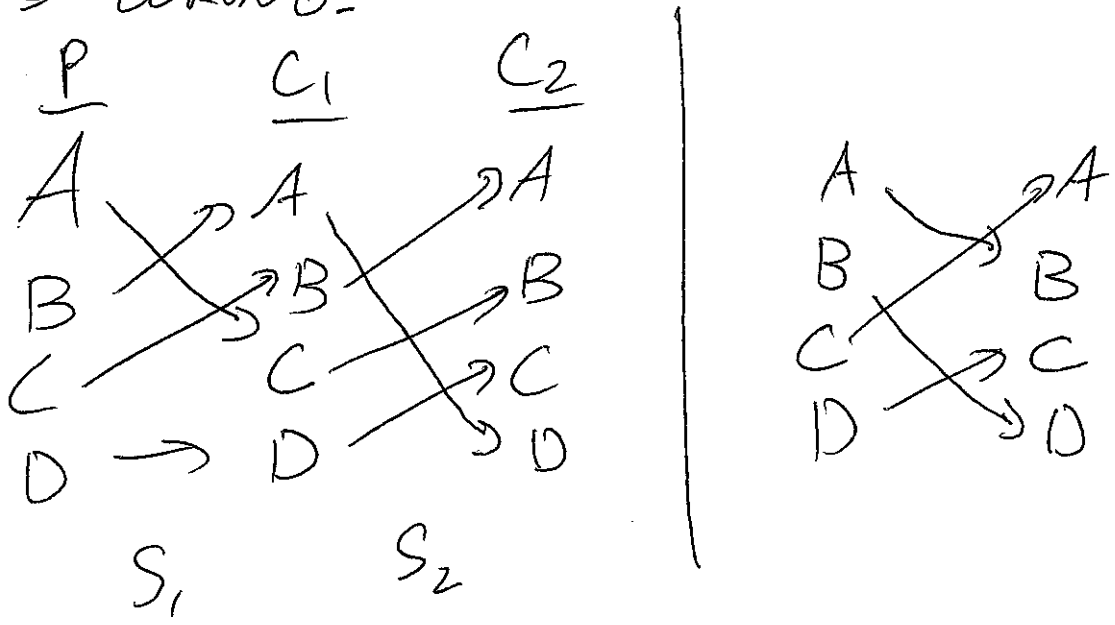
Based on partial information, you make guesses!

If some guess creates an impossibility, backtrack + try a different route.

TWO THINGS TO WATCH OUT FOR:

(1) RETRYING THE SAME COMBO.

(2) PLUGGING IN MULTIPLE LETTERS + INCORRECTLY GUESSING WHICH SUBSTITUTION IS WRONG.



4 null chars

20 code words

backspace char

100 symbols 00 → 99

'e' maps to 12

'a' = = 8

Vigenere

NOT BROKEN FOR 3 CENTURIES

Vigenere Cipher

Keyword: K N I G H T S
10, 13, 8, 6, 7, 19, 18

Plain: C R Y P T O G R A P H Y
2, 17, 24, 15, 19, 14, 6, 17, 0, 15, 7, 24
Key: 10 13 8 6 7 19 18 10 13 8 6 7
12 30 32 21 26 33 24 27 13 23 13 31
Cipher: M E G V A H Y B N X N F

$$C[i] = \left(P[i] + K[i \% K.length()] \right) \% 26$$

19th Century - reliably broken!

Kasiski Test -

find repeated N-grams in text, N ≥ 3.

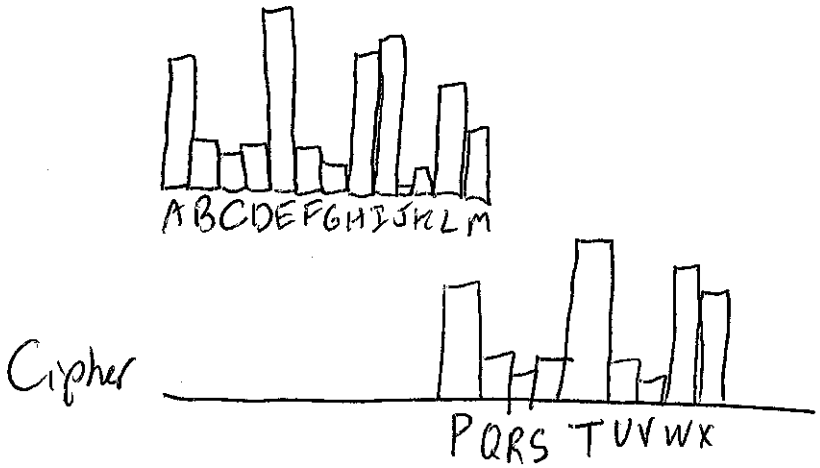
"QAP" 132 "QAP" 212 "QAP" 448

212 - 132 = 80
448 - 212 = 236
gcd(80, 236):

236 = 2×80 + 76
80 = 1×76 + 4
76 = 19×4

Keyword length allows you to "split up" the ciphertext letters into meaningful bins.

Frequency Chart English



Visual Soln: Shift each ciphertext bin to look like English freq.

Index of Coincidence:

Given a list of items $L_1, L_2, \ldots L_n$
What is the probability that 2 randomly chosen items in the list are the same?

choices 1st = n
choices 2nd = $(n-1)$
Sample Space = $n(n-1)$

All ways to choose 2 of the same letter $= f_a \times (f_a - 1) + f_b \times (f_b - 1) + \ldots + f_z (f_z - 1)$

$$= \frac{\sum_{i=0}^{25} f_i (f_i - 1)}{n(n-1)} = \frac{\sum_{CGLETTERS} f_c (f_c - 1)}{n(n-1)}$$

$$n = \sum_{CGLetters} f_c$$

$IC(\text{English}) = 0.0618$

$IC(\text{RandomLetters}) = \frac{1}{26} \sim .0384$ (LOWER)

Mutual Index of Coincidence

Given 2 sets of items, what is the probability an item chosen from the first set equals an item chosen from the second set.

$$f_0^+, f_1^+, f_2^+, f_3^+ \ldots + f_{25} = n$$

$$g_0^+, g_1^+, g_2^+, g_3 \ldots \quad g_{25} = m$$

$$\sum_{i=0}^{25} \frac{f_i \times g_i}{n \times m}$$

Set A = 10 As, 20 Bs, 15 Cs, 25 Ds = 70

Set B = 5 As, 25 Bs, 10 Cs, 10 Ds = 50

$$MIC(A,B) = \frac{10\times5 + 20\times25 + 15\times10 + 25\times10}{70 \times 50}$$

$$IC(A) = \frac{10\times9 + 20\times19 + 15\times14 + 25\times24}{70 \times 69}$$

① Calculate IC for k bins, assuming keyword length is k. If your guess

		A	B	C	D	E	
Shift = 1	Bin 1	5	20	15	25	5	70
	Bin 2	27	2	1	22	18	70
	Bin 3	30	4	4	19	13	70

Shifted 2 to the left

5	20	15	25	5
1	22	18	27	2
4	19	13	30	4

Bin 2 → 2
Bin 3 → 2

$5\times1 + 20\times22 + 15\times18 + 25\times27 + 5\times2$

$= 5 + 440 + 270 + 675 + 10$

$= 1115 + 285$

$= \boxed{1400}$

Key word : ACC
: BDD
: CEF
: DAA
: EBB

5	20	15	25	5
27	2	1	22	18

$135 + 40 + 15 + 550 + 90$

$175 + 565 + 90$

655
175
$\boxed{830}$

① I.C. of a set of letters