Practice02

Friday, March 10, 2023 1:51 PM

Breaking traditional ciphers (Shift/Vigenère)

1° Build distribution of letters in Moby Dick.

text deadbeef

alphabet d e a b f

2 3 1 1 1

8

2° Build the probability distribution of letters in the ciphertext

3° Comparing probability distributions of letters

p_i distribution of the language

q_i distribution of any text

$$\chi^2 = \sum_{i=1}^{c} \frac{(q_i - p_i)^2}{n_i}$$

(Chi-square)

4° Iterate over all possible shifts of cipher distribution, check χ^2 score against the language distribution and select the shift with lowest score.

(q_1, q_2, q_3, q_4)
(q_2, q_3, q_4, q_1)
(q_3, q_4, q_1, q_2)
(q_4, q_1, q_2, q_3)

VS (p_1, p_2, p_3, p_4)

Breaking Vigenere-cipher

1° Lenght of the key is known

0	1	2
3	4	5
6	7	

t: 0 1 2 3 4 5 6 7
i: 0 1 2 0 1 2 0 1

2° If we dont know the lengh of the key