Breaking Vigenére cipher

Recovering the length of the key

This is done with the Friedman method: Using the index of coincidence: $I_c(x) = \frac{\sum_{i=1}^{26} f_i(f_i-1)}{n(n-1)} \approx \sum_{i=1}^{26} p_i^2$ Where: - n is the length of the text. - f_i is the frequency of the i-th letter (i.e. the number of times it occurs in a text) - p_i is the probability of the i-th letter, $p_i = \frac{f_i}{n}$, this gives the probability that two letters, randomly chosen from a text, are the same. [[index-of-coincidence.png]] The value of the index of coincidence can range from $\frac{1}{26}$ (if the letters have the same probability, basically random text) to 1 (single letter text e.g. AAAAA). After computing the I_c, if the value is ≈ 0.038, we're trying to break a poly alphabetic cipher; if the value is ≈ 0.065, we're trying to break a mono alphabetic cipher. (I believe this is assuming we're using the English language).

Recovering the key