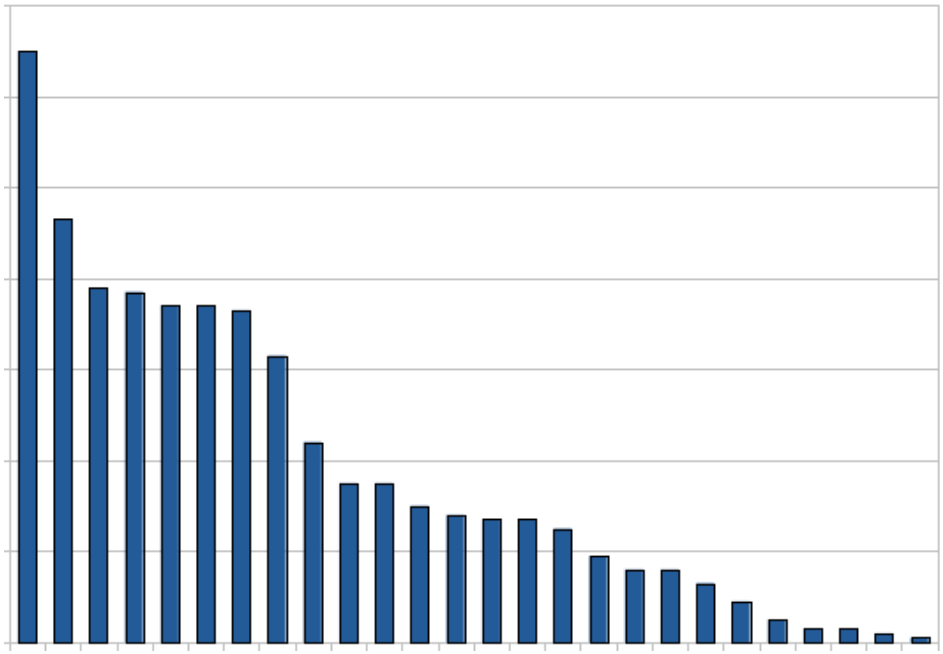
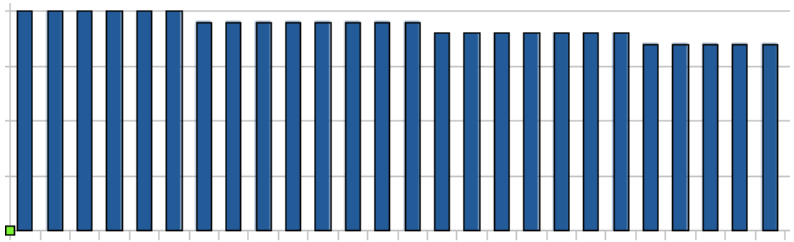
How to break the ADFGVX cipher

1. guess at the size of the permutation key (key 2)

2. Align columns next to each other and test numbers of the ADFGVX pairs that appear. Sort them in decreasing number.



English



not English

Keep only pairs that 'look like' English distribution of letters

To test if a distribution looks like English

Use this to tell which columns are next to each other

Recall:

$$\sum_i p_i log(q_i) \leq \sum_i p_i log(p_i)$$

Sort the probabilities and compute:

$$\sum_i p_{Eng_i} log(p_i)$$

$$p_i \approx p_{Eng_i} \qquad\qquad p_i \approx \frac{1}{26}$$

$$\sum_i p_{Eng_i} log(p_{Eng_i}) = -2.88 \qquad\qquad \sum_i p_{Eng_i} log(1/26) \approx -3.26$$

Our cyphertext is now roughly equivalent to breaking a monoalphabetic substitution + rectangular transposition cipher

Each letter of the alphabet is replaced by a pair of letters

Apply 'Metropolis' algorithm to break? Maybe some modified version, but the scoring function in the metropolis algorithm required that we compare double letter statistics, but we have columns of rectangle scrambled.

Apply rectangular transposition algorithm? Maybe some modified version, but the table of values we computed relied on the comparison alphabet being English.