aabc
aabc

Autocorrelation

Correlates text with shifted versions of itself

- Autocorrelation
- Description
- Background

Text to analyze

Restrict to German alphabet

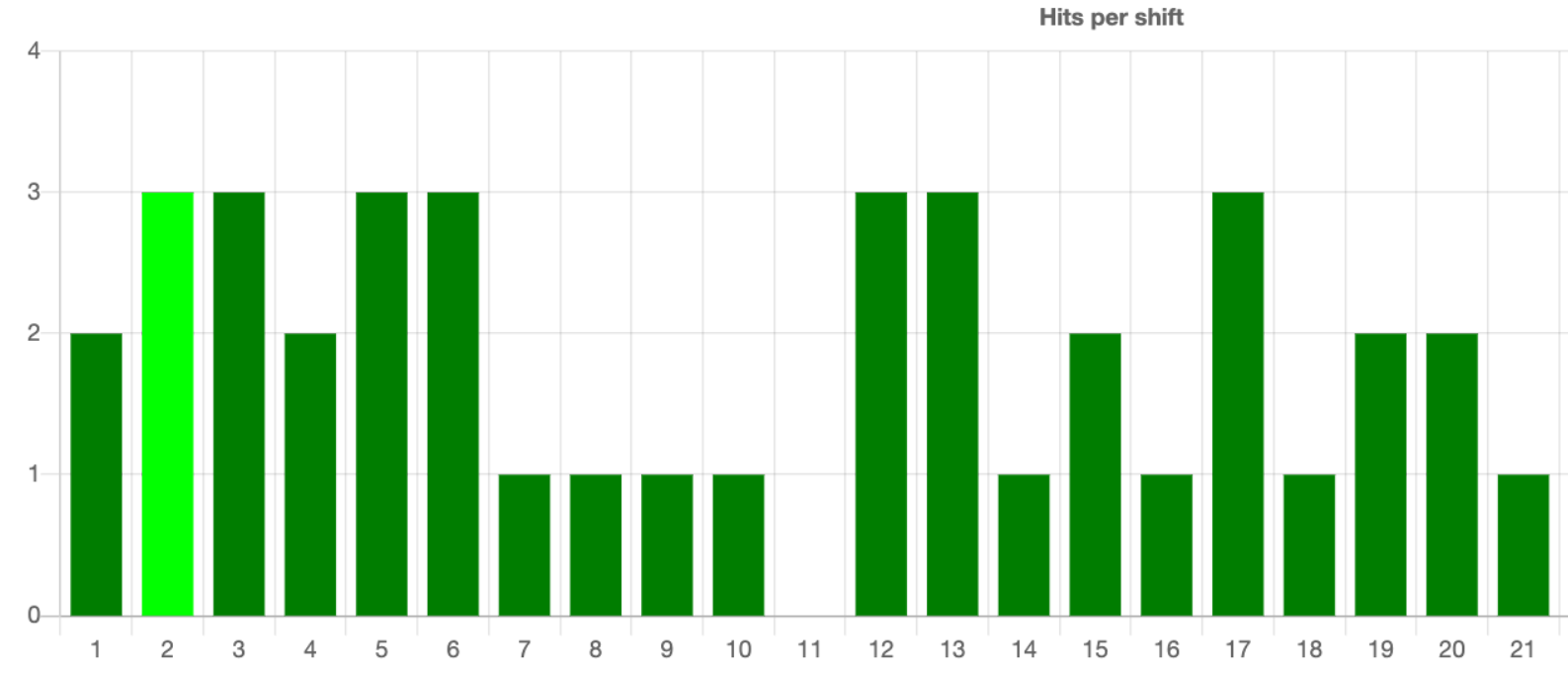
English German

ALRTRHBASHLUSENHEREAAEC
LTCMHIJNDHEIENGG

Text length: 39

Shift by: 2 (click on a bar below to change the shift value)
alrtrhbashlusenhereaaecltcmhijndheiengg

Number of bars: 30



Author: Jean Michel Polak

ocorrelation compares a text with moved copies of the same text. In each case the matching character etermined. The number of hits per shift is then displayed in the diagram. You can choose between the man and English alphabet. Only the letters of the selected alphabet are analyzed. The number of shifts ends on the length of the text (you can shift a text of n characters by a maximum of n, then they are of below each other).

The shifts are controlled by clicking on the bars in the diagram.

You want to analyze the sentence 'Hello, how are you doing?' with a shift of 2. Characters not belonging to the alphabet such as '?', comma and spaces are filtered out.

```
Orginal text:       Hello, how are you doing?

Modified:         hellohowareyoudoing
Shifted by 9:               hellohowareyoudoing
```

The shift by 9 therefore has 2 matches.

Reference

● **Chart.js** (used for diagram)

Autocorrelation is based on the assumption that, on the one hand, certain characters occur repeatedly in plaintext, and on the other hand, these characters are occasionally encoded by the same letters of the keyword. This leads to the assumption that the probability of matches between ciphertext and shifted ciphertext would have to be the highest if the key length were shifted by a multiple of the key length.

For example, the Vigenère cipher can be cracked. The periodically recurring maximum values of the number of matching characters, indicate the key length of the Vigenère cipher.

Autocorrelation analysis is more efficient and much more illustrative than the Friedman or Kasiski test. It is versatile and is also used in signal processing.

Since the autocorrelation is a complex calculation, it is recommended that larger texts be processed with a locally installed program like CrypTool2 (**https://www.cryptool.org/en/cryptool2**).

Reference

● Autocorrelation: **https://en.wikipedia.org/wiki/Autocorrelation**

Share link