

PicoCTF19 La Cifra De - Capture The Flag

Capture The Flag

PicoCTF19 La Cifra De

Challenge

I found this cipher in an old book. Can you figure out what it says? Connect with 'nc 2019shell1.picoctf.com 12254'.

Hints

There are tools that make this easy.

Perhaps looking at history will help

Solution

```
$ nc 2019shell1.picoctf.com 12254
```

Encrypted message:

```
Ne iy nytkwpsznyg nth it mtsztcy vjzprj zfzjy rkhpibj nrkitt ltc tnnygy ysee itd tte cxjltk
```

Ifrosr tnj noawde uk siyyzre, yse Bnretèwp Cousex mls hjpn xjtnbjytki xatd eisjd

Iz bls lfwsqkj azycihzeej yz Brftsk ip Volpnèxj ls oy hay tcimnyarqj dknroqpd os 1553 my Mnzvgs Mazytszf Merqlsu ny hox moup Wa inqrg ipl. Ynr. Gotgat Gltzndtg Gplrfd

Ltc tnj tmvqpmkseaznzn uk ehox nivmpr g ylbrj ts ltcмки my yqtdosr tnj wocjc hgqq ol fy oxitngwj arusahje fuw ln gaaaxjytrd catizm tzxbkw zf vqlckx hizm ceyupcz yz tnj

Ehk ktryy herq-ooizxetypd jjdcxnatoty ol f aordllvmlbkytc inahkw socjgex, bls sfoe gwzuti 1467 my Rjzn Hfetoxea Gqmexyt.

Tnj Gimjyèrk Htpnjc iy ysexjqoxj dosjeisjd cgqwej yse Gqmexyt Doxn ox Fwbkwei Inahkw.

Tn 1508, Ptsatsps Zwttnjxiar tnbjytki ehk xz-cgqwej ylbaql rkhea (g rltxni ol xsilypd gqahggpty) ysaz bzuri wazjc bk f nroytcgq nosuznkse ol yse Bnretèwp Cousex.

Gplrfdoy xpcuso butvlky lpvjlrki tn 1555 gx l cuseitzltoty ol yse lncsz. Yse rthex mllbjd ol yse gqahggpty fce tth snnqtki cemzaxqj, bay ehk fwpnfmezx lnj yse osoed

Well could be a substitution cipher or any other, lets try our tools:

<https://www.guballa.de/vigenere-solver>

It is interesting how in history people often receive credit for things they did not create

During the course of history, the Vigenère Cipher has been reinvented many times

It was falsely attributed to Blaise de Vigenère as it was originally described in 1553 by Giovan Battista Bellaso in his book La cifra del. Sig. Giovan Battista Bellas

For the implementation of this cipher a table is formed by sliding the lower half of an ordinary alphabet for an apparently random number of places with respect to the

The first well-documented description of a polyalphabetic cipher however, was made around 1467 by Leon Battista Alberti.

The Vigenère Cipher is therefore sometimes called the Alberti Disc or Alberti Cipher.

In 1508, Johannes Trithemius invented the so-called tabula recta (a matrix of shifted alphabets) that would later be a critical component of the Vigenère Cipher.

Bellaso's second booklet appeared in 1555 as a continuation of the first. The lower halves of the alphabets are now shifted regularly, but the alphabets and the index

It worked... we see: picoCTF{b311a50_0r_v1gn3r3_c1ph3ra653edec}

Flag

picoCTF{b311a50_0r_v1gn3r3_c1ph3ra653edec}