

La cifra de: Points(200)

Description- I found this cipher in an old book. Can you figure out what it says?

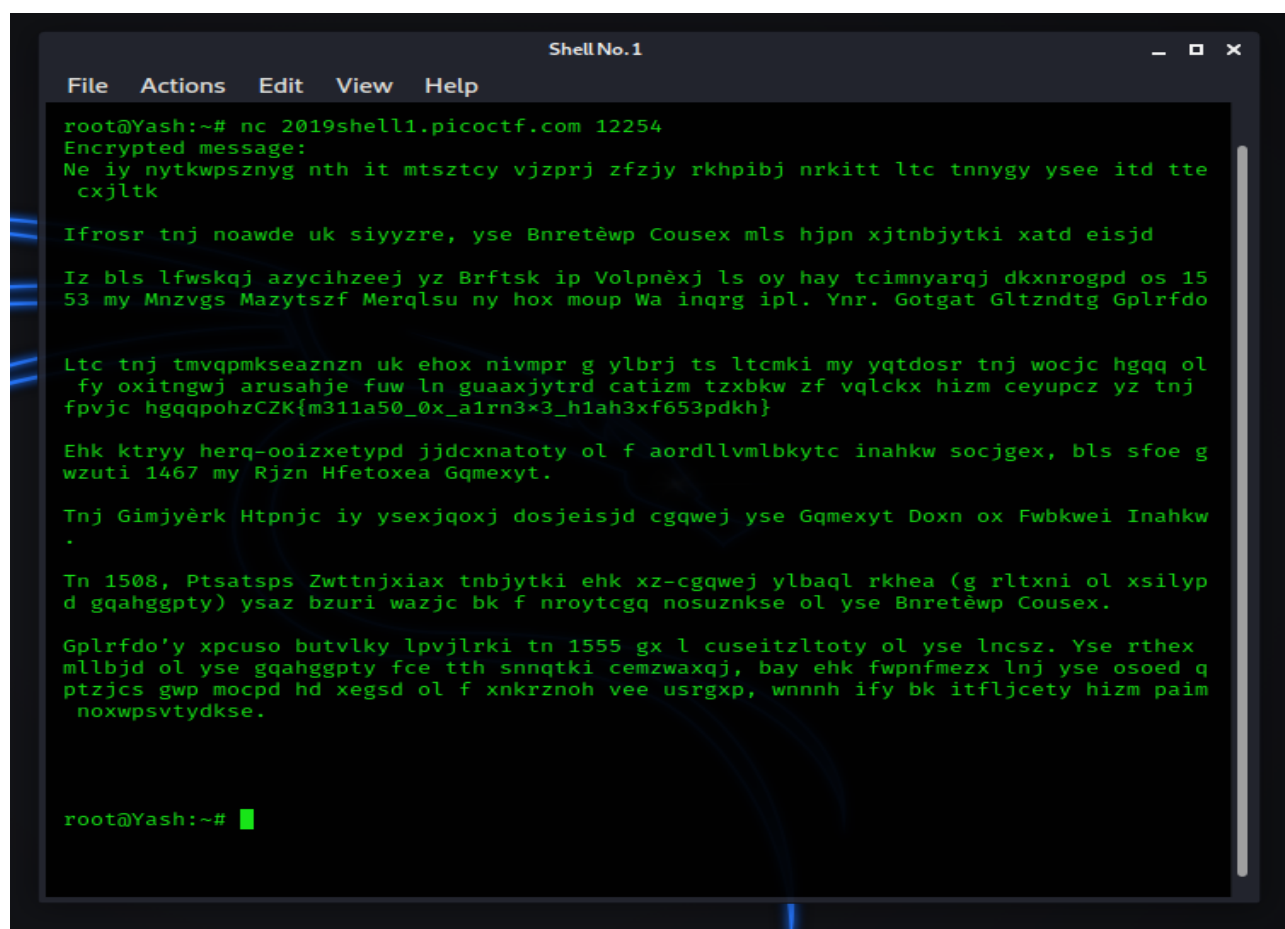
Connect with nc 2019shell1.picoctf.com 12254 .

Hint- There are tools that make this easy.

Perhaps looking at history will help.

Solution-

We connect to the server and get



```
root@Yash:~# nc 2019shell1.picoctf.com 12254
Encrypted message:
Ne iy nytkwpsznyn nht 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 15
53 my Mnzvgs Mazytszf Merqlsu ny hox moup Wa inqrg ipl. Ynr. Gotgat Gltzndtg Gplrfd

Ltc tnj tmvqpmksezazn uk ehox nivmpr g ylbrj ts ltcnki my yqtdosr tnj wocjc hgqq ol
fy oxitngwj arusahje fuw ln guaaxjytrd catizm tzxbkw zf vqlckx hizm ceyupcz yz tnj
fpvjc hgqqpohzCZK{m311a50_0x_a1rn3x3_h1ah3xf653pdkh}

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

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

Tn 1508, Ptsatsps Zwttnjxiat tnbjytki ehk xz-cgqwej ylbaql rkhea (g rltxni ol xsilyp
d 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
mlbjd ol yse gqahggpty fce tth snnqtki cemzwxqj, bay ehk fwpnfmezx lnj yse osoed q
ptzjcs gwp mocpd hd xegsd ol f xnkzrnoh vee usrgxp, wnnnh ify bk itfljcety hizm paim
noxwpsvtydkse.

root@Yash:~# curl -s https://picoctf.com/api/challenges/2019shell1/p12254
{"challenge": "La cifra de: Points(200)", "description": "I found this cipher in an old book. Can you figure out what it says?", "hint": "There are tools that make this easy. Perhaps looking at history will help.", "solution": "We connect to the server and get", "type": "Points", "value": "200"}
```

The encrypted message is:

Ne iy nytkwpsznyg nth it mtsztcy vjzprj zfzjy rkhipibj 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 Gplrfdo

Ltc tnj tmvqpmkseaznzn uk ehox nivmpr g ylbrj ts ltcмки my yqtdosr tnj wocjc hgq q ol fy oxitngwj arusahje fuw ln guaaxyjtrd catizm tzxbkw zf vqlckx hizm ceyupcz yz tnj fpvjc hgqqpohzCZK{m311a50_0x_a1rn3x3_h1ah3xf653pdkh}

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

Gplrfdo'y xpcuso butvlky lpvjlрки tn 1555 gx l cuseitzltoty ol yse lncsz. Yse rthex mllbjd ol yse gqahggpty fce tth snnqtki cemzwaxqj, bay ehk fwpnfmez x lnj yse osoed qptzjcs gwp mocpd hd xegsd ol f xnrkrznoh vee usrgxp, wnnnh ify bk itfljcety hizm paim noxwpsvtydkse.

From the description of the challenge and the encrypted message, we got to know that it's Vignere Cipher.

But in Vignere Cipher we need a key to decode.

After searching for vignere cipher decoder without key, I got [this](#) site in which we can decode Vignere Cipher without knowing the key.

After decoding I got the decoded message and the flag.

Decoded message:

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 Bellaso

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 upper halfpicoCTF{b311a50_0r_v1gn3r3_c1ph3ra653edec}

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 letters are mixed by means of a mnemonic key phrase, which can be different with each correspondent.

The flag is: picoCTF{b311a50_0r_v1gn3r3_c1ph3ra653edec}