

Mark Seliternikov

picoCTF - waves over lambda [300 points]

```
mark@mark-ubuntu:~$ nc jupiter.challenges.picoctf.org 43522
-----
e1sxufoy vlul zy htau brfx - bulpalseh_zy_e_1clu_rfgdqf_txbgfasufb
-----
frlwLh bhqitueiozoev tfufgfkic jfy ovl ovzuq yis ib bhqiu nfcriczoev tfufgfkic,
f rfsq ijslu jlrr tsijs zs iau qzyouzeo zs vzy ijs qfh, fsq yozrr ulgldlulq fgi
sx ay ijszx ot vzy xriigh fsq ourfxze qlfov, jvzev vfnnlslq ovzuolls hlufy fxi, f
sq jvzev z yvrrr qlyeuzdl zs zoy nutlu nrfel. biu ovl nulylso z jzrr isrh yfh o
vfo ovzy rfsqijslubiu yi jl aylq ot efrr vzg, froviavx vl vfugrh yniso f qfh ib
vzy rzbl is vzy ijs lyofoljfy f youfsxl ohnl, hlo isl nulooh bulpalsorh ot dl gl
o jzov, f ohnl fdmleo fsq czetlay fsq fo ovl yfgl ozgl ylsylrlly. dao vl jfy isl
ib ovilyl ylsylrlly nluyisy jvl ful cluh jlrr efnrdl ib riltzxs fbolu ovizu jtu
rarh fbbfzuy, fsq, fnnfulsorh, fbolu stovzxs lryl. bhqiu nfcriczoev, biu zsyofs
el, dlxfz jzov slwo ot stovzxs; vzy lyofol jfy ib ovl ygfrrlyo; vl ufs ot qzsl f
o iovlu gls'y ofdrly, fsq bfyolslq is ovlg fy f oifqh, hlo fo vzy qlfov zo fnnlf
ulq ovfo vl vfq f vasqulq ovlayfsq uiadrly zs vfug efyv. fo ovl yfgl ozgl, vl jf
y frr vzy rzbl isl ib ovl giyo ylsylrlly, bfsofyozevr blrrijy zs ovl jvirl qzyou
zeo. z ulnlfo, zo jfy sio yoanzqzohovl gfmuzoh ib ovlyl bfsofyozevr blrrijy ful
yvuljq fsq zsolrrzxiso lsiavdao mayo ylsylrlyyslyy, fsq f nlearzfu sfosisfr bi
ug ib zo.
```

לאתגר זה מקבלים כתובת ופורט שניתן להקשיב באמצעות NetCat.

זה הפלט שמקבלים.

We made a lot of substitutions to encrypt this. Ca

לאתגר זה כתוב ב-description את הדבר הבא:

אז מיד לאחר שהבנתי את הרמז חיפשתי באינטרנט "substitution decryptor" (לא הכרתי מה זה באותו זמן).

מתברר שזו שיטת הצפנה שכל העניין שלה זה להחליף אות מסוימת באות אחרת (אקראית).

הדרך שהאתר שמצאתי מפענח מה הוא "המפתח" של ההצפנה הוא לפי התדירות של הופעת האותיות בשפה האנגלית ובטקסט (כנראה גם עוד חישובים כמו מציאת מילים הגיוניות וכו'). כנראה בגלל זה דאגו שיהיה טקסט ארוך כדי להקל על החישוב (יש יותר מידע לעבוד איתו)

קישור לאתר: <https://planetcalc.com/8047>

עכשיו כל מה שעליי לעשות זה למצוא את התוכן הלא מוצפן.

הנה הטקסט הלא מוצפן, (כדי שהדגל יהיה נכון צריך להמיר לאותיות קטנות)

CONGRATS HERE IS YOUR FLAG - FREQUENCY_IS_C_OVER_LAMBDA_OGfMAUNRAF

ALEXEY FYODOROVITCH KARAMAZOV WAS THE THIRD SON OF FYODOR PAVLOVITCH KARAMAZOV, A LAND OWNER WELL KNOWN IN OUR DISTRICT IN HIS OWN DAY, AND STILL REMEMBERED AMONG US OWING TO HIS GLOOMY AND TRAGIC DEATH, WHICH HAPPENED THIRTEEN YEARS AGO, AND WHICH I SHALL DESCRIBE IN ITS PROPER PLACE. FOR THE PRESENT I WILL ONLY SAY THAT THIS LANDOWNERFOR SO WE USED TO CALL HIM, ALTHOUGH HE HARDLY SPENT A DAY OF HIS LIFE ON HIS OWN ESTATEWAS A STRANGE TYPE, YET ONE PRETTY FREQUENTLY TO BE MET WITH, A TYPE ABJECT AND VICIOUS AND AT THE SAME TIME SENSELESS. BUT HE WAS ONE OF THOSE SENSELESS PERSONS WHO ARE VERY WELL CAPABLE OF LOOKING AFTER THEIR WORLDLY AFFAIRS, AND, APPARENTLY, AFTER NOTHING ELSE. FYODOR PAVLOVITCH, FOR INSTANCE, BEGAN WITH NEXT TO NOTHING; HIS ESTATE WAS OF THE SMALLEST; HE RAN TO DINE AT OTHER MEN'S TABLES, AND FASTENED ON THEM AS A TOADY, YET AT HIS DEATH IT APPEARED THAT HE HAD A HUNDRED THOUSAND ROUBLES IN HARD CASH. AT THE SAME TIME, HE WAS ALL HIS LIFE ONE OF THE MOST SENSELESS, FANTASTICAL FELLOWS IN THE WHOLE DISTRICT. I REPEAT, IT WAS NOT STUPIDITYTHE MAJORITY OF THESE FANTASTICAL FELLOWS ARE SHREWD AND INTELLIGENT ENOUGH BUT JUST SENSELESSNESS, AND A PECULIAR NATIONAL FORM OF IT.