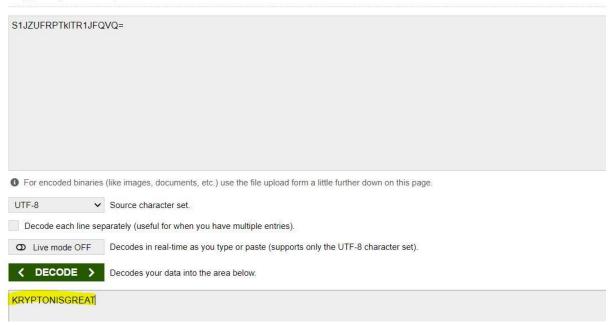
## Krypton:

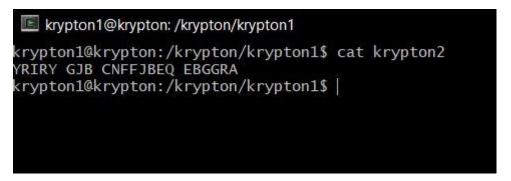
The level0 was easy all I had to do is just convert the encrypt base64 string to ASCII and I got the password to the next level.

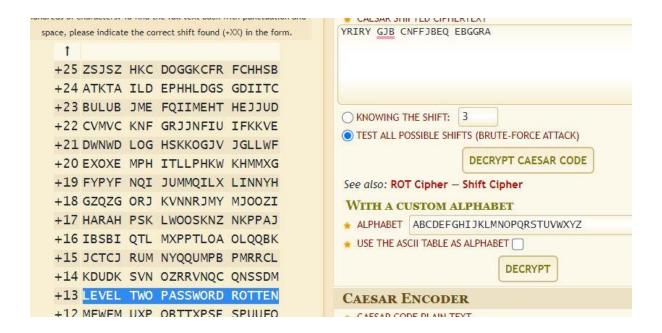
## Decode from Base64 format

Simply enter your data then push the decode button.



For Level1 I looked at the file krypton2 and the hints were clear that it's a Caesar Cipher, so I looked at all the shift value and found the password of the next level.



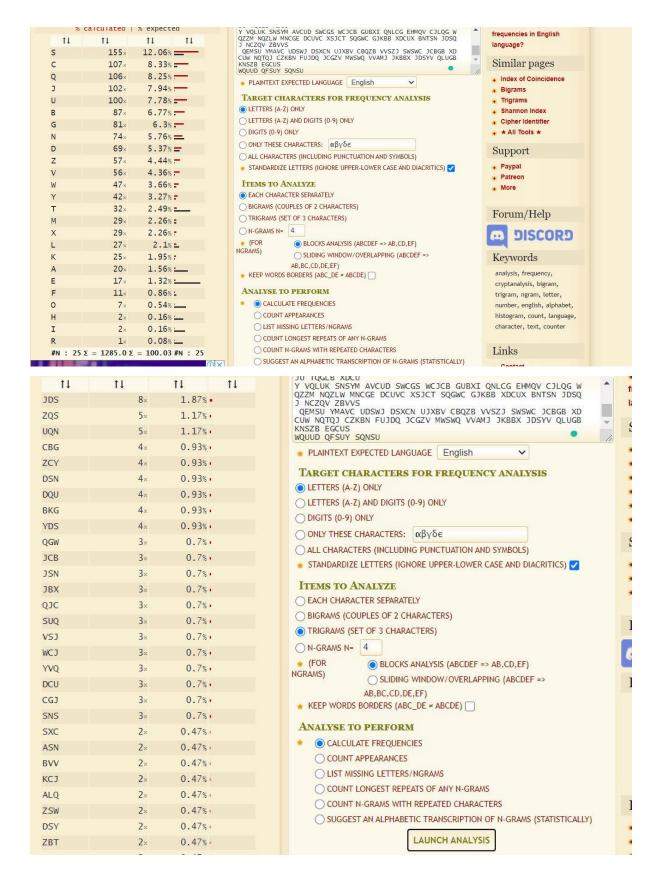


For this level, I was given a program encrypt which encrypts the file with the same key for the cipher of password krypton3, so I followed the step of creating a different directory and run the encrypt program on A-Z and I got the key for the cipher, and I was able to decrypt the password, if I did the same thing for the previous stage, I would still get the password.

```
cat: keyfile.dat: Permission denied
krypton2@krypton:/tmp/tmp.i2M0kLWEkW$ echo "ABCDEFGHIJKLMNOPQRSTUVWXYZ" > text
krypton2@krypton:/tmp/tmp.i2M0kLWEkW$ cat text
ABCDEFGHIJKLMNOPQRSTUVWXYZ
krypton2@krypton:/tmp/tmp.i2M0kLWEkW$ /krypton/krypton2/encrypt text
krypton2@krypton:/tmp/tmp.i2M0kLWEkW$ ls
ciphertext keyfile.dat text
krypton2@krypton:/tmp/tmp.i2M0kLWEkW$ cat ciphertext
MNOPQRSTUVWXYZABCDEFGHIJKLkrypton2@krypton:/tmp/tmp.i2M0kLWEkW$ |

MNOPQRSTUVWXYZABCDEFGHIJKLkrypton2@krypton:/tmp/tmp.i2M0kLWEkW$
krypton2@krypton:/tmp/tmp.i2M0kLWEkW$ cat /krypton/krypton2/
encrypt keyfile.dat krypton3 README
krypton2@krypton:/tmp/tmp.i2M0kLWEkW$ cat /krypton/krypton3 | tr "[A-Z]" "[M-ZA-L]"
AYCQYPGQCYOW
krypton2@krypton:/tmp/tmp.i2M0kLWEkW$ cat /krypton/krypton2/krypton3 | tr "[M-ZA-L]" "[A-Z]"
GAESARISEASY
krypton2@krypton:/tmp/tmp.i2M0kLWEkW$ cat /krypton/krypton2/krypton3 | tr "[M-ZA-L]" "[A-Z]"
GAESARISEASY
krypton2@krypton:/tmp/tmp.i2M0kLWEkW$ cat /krypton/krypton2/krypton3 | tr "[M-ZA-L]" "[A-Z]"
GAESARISEASY
krypton2@krypton:/tmp/tmp.i2M0kLWEkW$ |
```

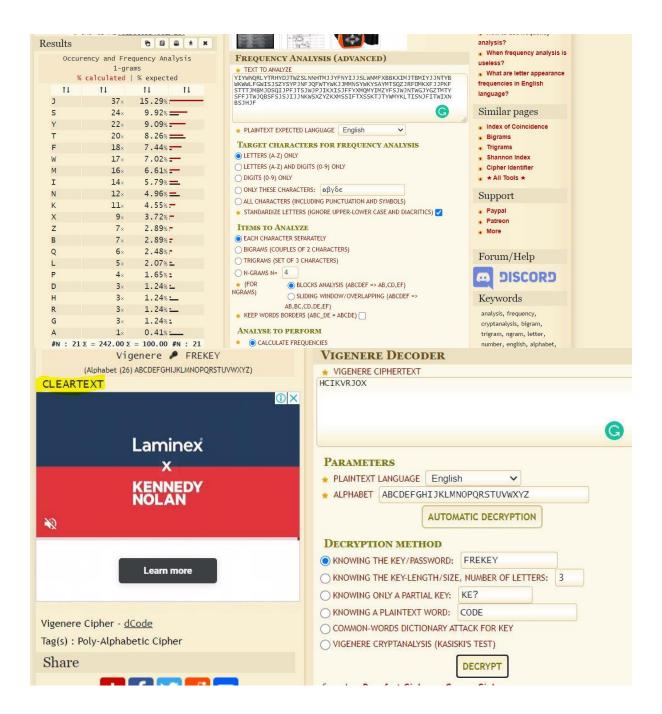
For Leve4, the hint was given to do frequency analysis, so I used an online tool for frequency analysis and the result I found for 1 character and a group of 3 characters was:



After this, I just started to guess as the most common letter in English is E so I replace E with S and the most common word is THE so I replace THE with JDS. And for doing a bunch of guesses the string started to make sense and I got the password for the next level.

```
KEVWW BGETH EVEIE VXBMN YQUUK BNWCU ANMTE krypton30krypton:/krypton/krypton35 cat krypton4 | tr "[JDSQ]" "[THEA]"
KEVWW BGETH EVEIE VXBMN YAUUK BNWCU ANMTE krypton30krypton:/krypton35 cat krypton4 | tr "[JDSQG]" "[THEA]"
KEVWW BOETH EVEIE VXBMN YAUUK BNWCU ANMTE krypton30krypton:/krypton35 cat krypton4 | tr "[JDSQG]" "[THEAO]"
KEVWW ONETH EVEIE VXBMN YAUUK ONWCU ANMTE Krypton30krypton:/krypton36 cat krypton4 | tr "[JDSQGG]" "[THEAON]"
KEVWW ONETH EVEIE VXOMN YAUUK ONWCU ANMTE Krypton30krypton:/krypton35 cat krypton4 | tr "[JDSQGGW]" "[THEAONLW]"
KELLW ONETH ELEIE LXONN YAUUK ONWCU ANMTE Krypton30krypton:/krypton35 cat krypton4 | tr "[JDSQGGW]" "[THEAONLW]"
KELLW ONETH ELEIE LXONN YAUUK ONWCU ANMTE Krypton30krypton:/krypton36 cat krypton4 | tr "[JDSQGGW]" "[THEAONLW]"
KELLW ONETH ELEIE LXONN YAUUW ONWCU ANMTE Krypton30krypton:/krypton36 cat krypton4 | tr "[JDSQGGWM]" "[THEAONLW]"
KELLW ONETH ELEIE LXONN YAUUW ONWCU ANMTE Krypton30krypton:/krypton36 cat krypton4 | tr "[JDSQGGWM]" "[THEAONLW]"
KELLW ONETH ELEIE LXONN YAUWW ONWCU ANMTE Krypton30krypton:/krypton36 cat krypton4 | tr "[JDSQGGWM]" "[THEAONLW]" | tr "[JDSQGGWMI]" "[THEAONLW]" "[THEAONLWDS]" | tr "[JDSQGGWMI]" "[THEAONLWDSPRISFU]" | tr "[JDSQGGWMI]" "[THEAONLWDSPRISFU]" | tr "[JDSQGGWMI]" "[THEAONLWDSPRISFU]" | tr "[JDSQGGWMI]" "[THEAONLWDSPRISFU]" | tr "[JDSQGGWMI]" "[THEAONLWDSP
```

For Leve5, it was a poly-alphabetic cipher called Vigenère cipher so after doing some research on the cipher I got an idea on how to decrypt it, this video really helped full in understanding the cipher decryption trick (<a href="https://www.youtube.com/watch?v=LaWp\_Kq0cKs">https://www.youtube.com/watch?v=LaWp\_Kq0cKs</a>), I wrote a python script which only reads the letter give as input from the key so I can do frequency analysis on it as it has been decrypted with the same key. Doing this I can figure out the letter used to decrypt, and repeating this I got the entire key.



So for Level6, the key length was not given so I had to follow the video

(https://www.youtube.com/watch?v=LaWp\_KqOcKs), about the Vigenère cipher and I wrote a python which counts the coincidence, and use the output from the python program I found 9 and its factor have a higher rate of co-incidence for this I need to ignore 1,2, and 3 as they are the factor for most of the number.

```
PS C:\Users\UZAIF SHAIKH\Documents\Python Scripts> python .\vigenere.py

1 : 14
2 : 10
3 : 15
4 : 16
5 : 6
6 : 13
7 : 10
8 : 17
9 : 15
10 : 18
11 : 15
12 : 12
13 : 10
14 : 14
15 : 12
16 : 13
17 : 14
18 : 10
19 : 15
20 : 14
```

And after guessing the key length I followed the same method from the previous level and got the key (this took me a lot of time achy) and the key was KEYLENGTH, and I used the online tool to get decrypt the cipher.



For the last level, I read the readme file and found out that that have been using XOR to encrypt the plaintext so to find how the key, there is a property of XOR that  $A \land B = C$  and if  $A \land C = B$  so using strings of A and to encrypt with give us the key and after getting the key I just ran the Vigenère cipher decrypt and got the password.

