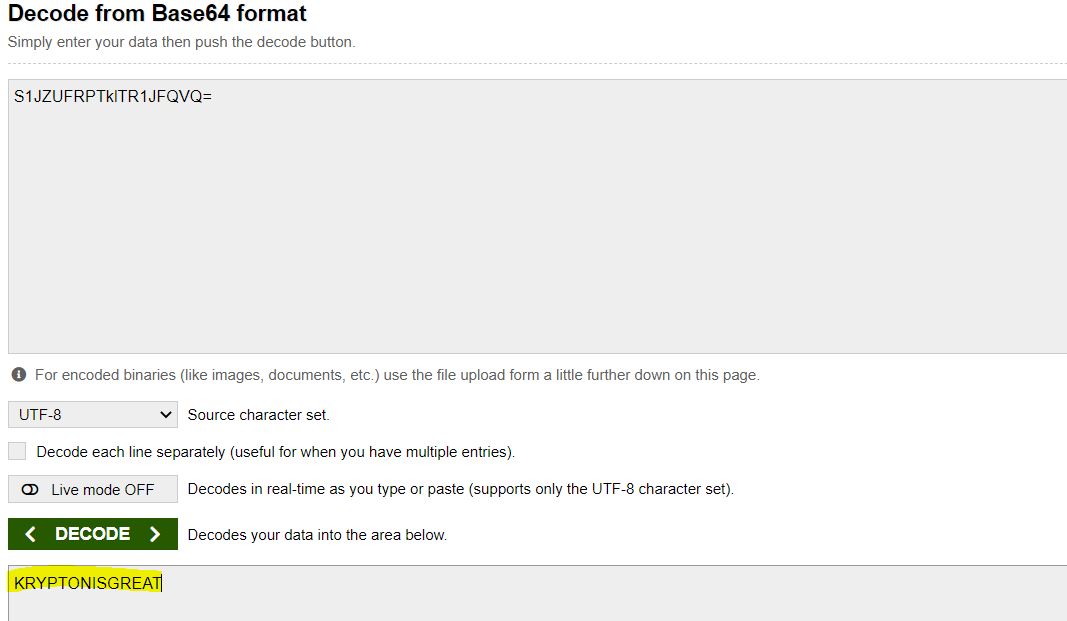
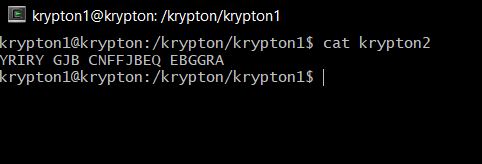
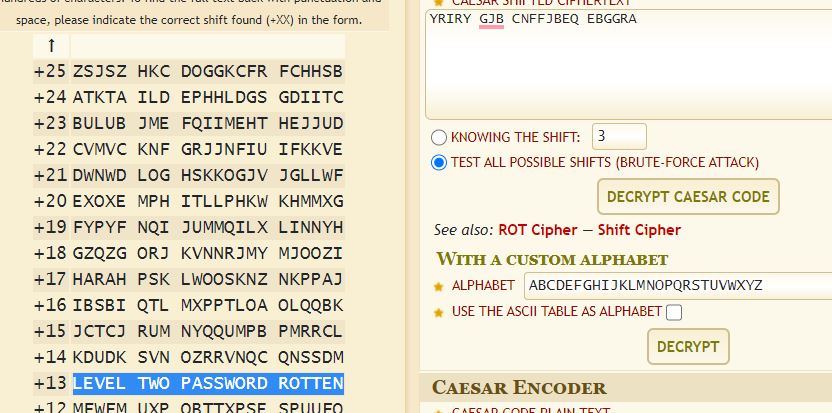
**Krypton:**

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.

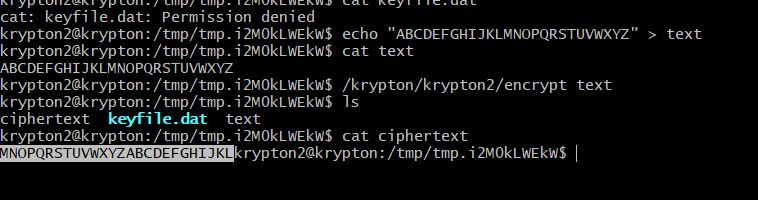


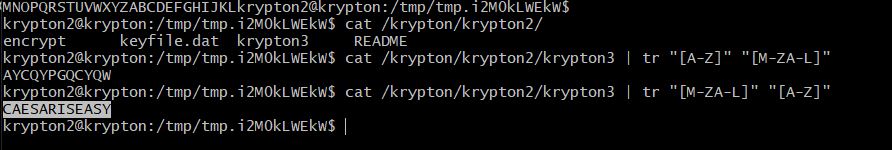
For Level1 I looked at the file krypton2 and the hints were clear that it’s a Caesar Cipher, so I looked at all the shift value and found the password of the next level.



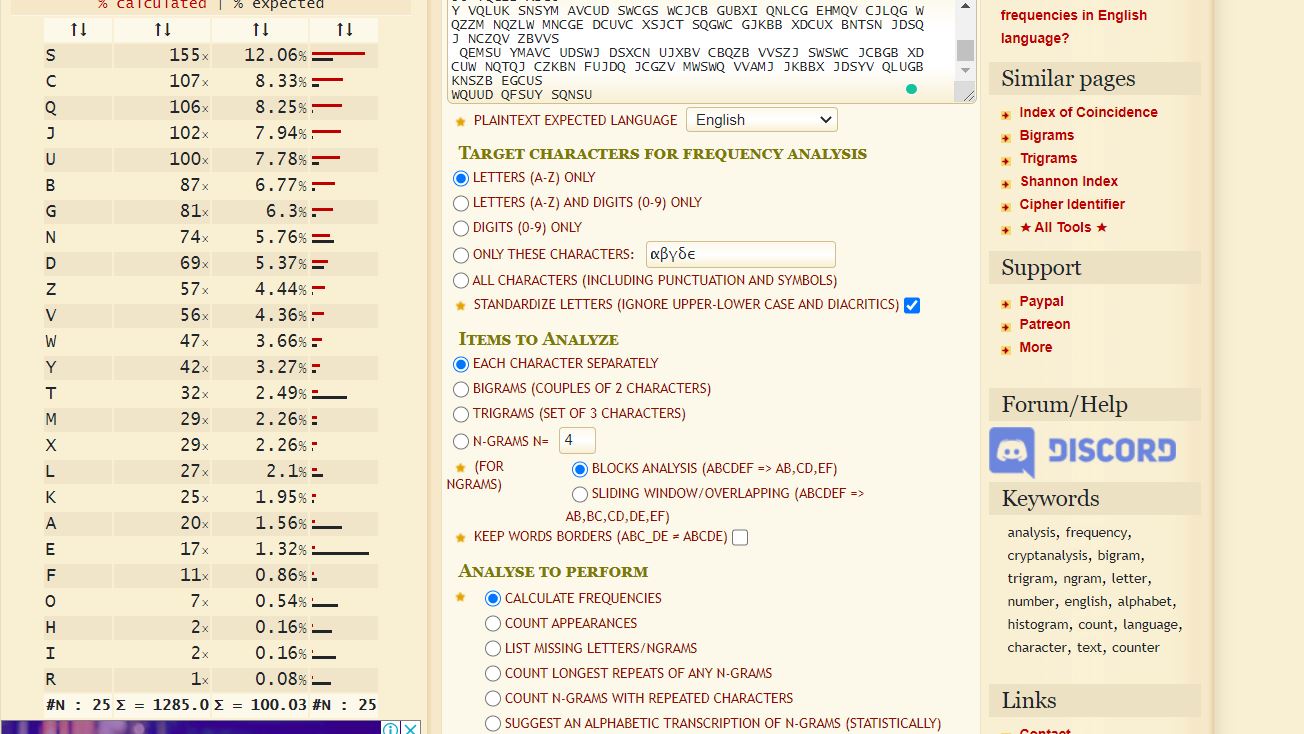


For this level, I was given a program encrypt which encrypts the file with the same key for the cipher of password krypton3, so I followed the step of creating a different directory and run the encrypt program on A-Z and I got the key for the cipher, and I was able to decrypt the password, if I did the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



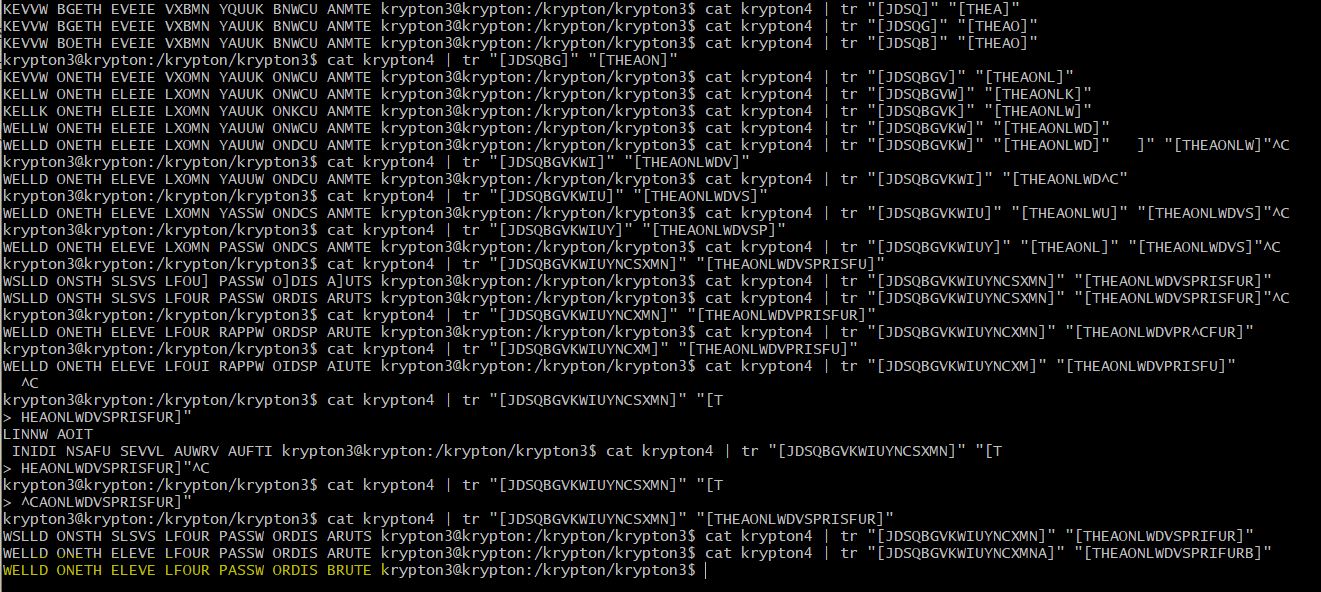


For Leve4, the hint was given to do frequency analysis, so I used an online tool for frequency analysis and the result I found for 1 character and a group of 3 characters was:

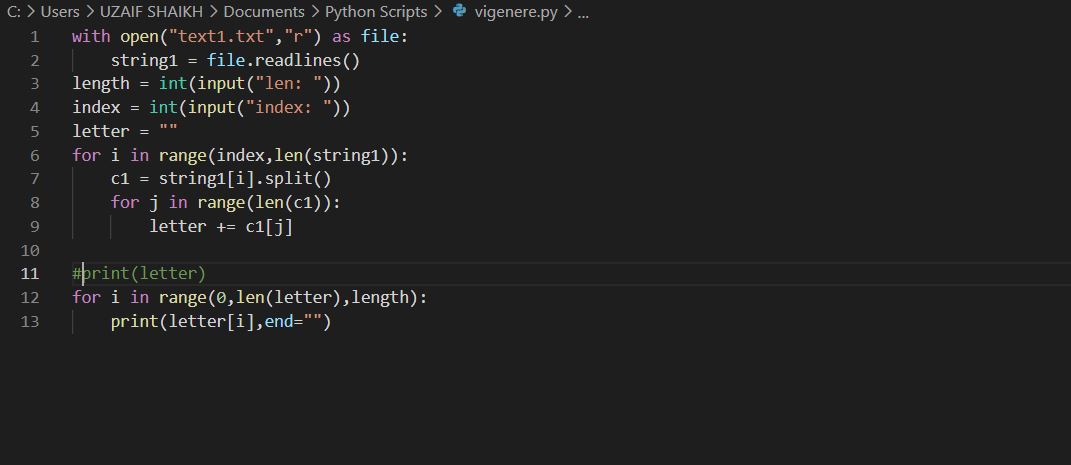


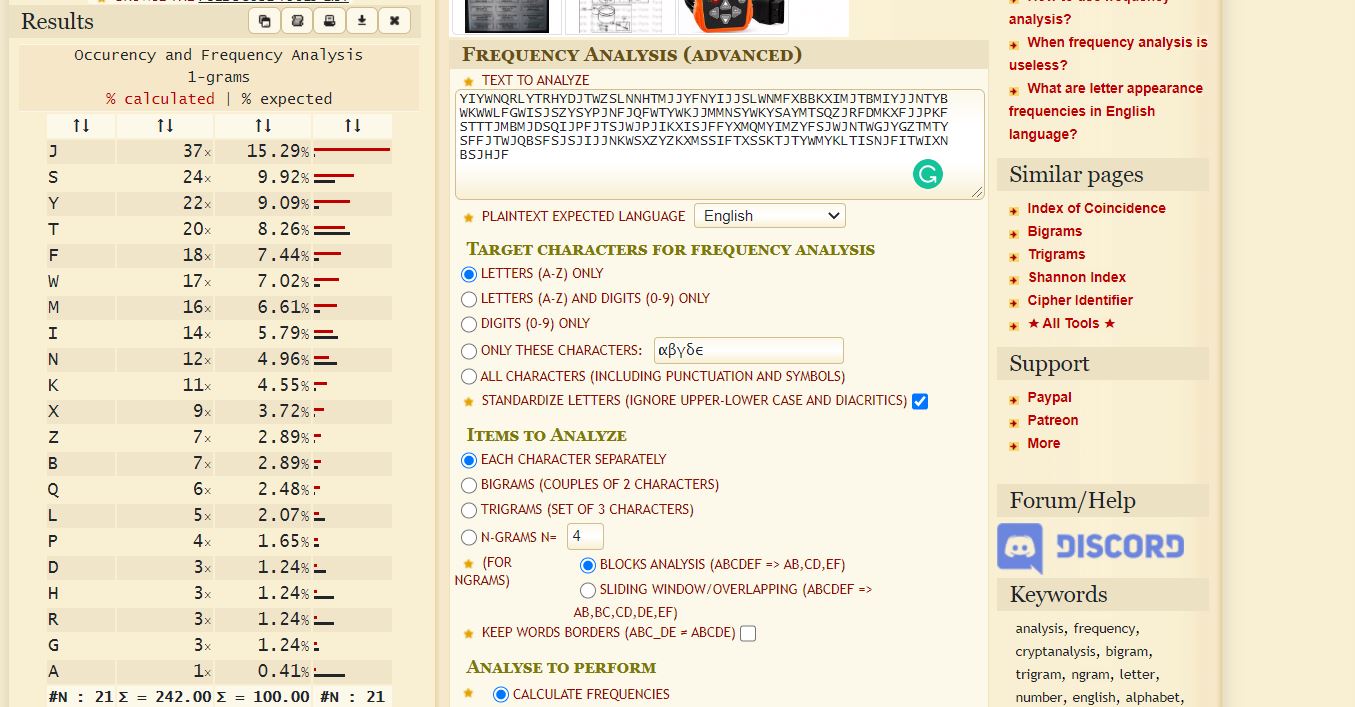


After this, I just started to guess as the most common letter in English is E so I replace E with S and the most common word is THE so I replace THE with JDS. And for doing a bunch of guesses the string started to make sense and I got the password for the next level.

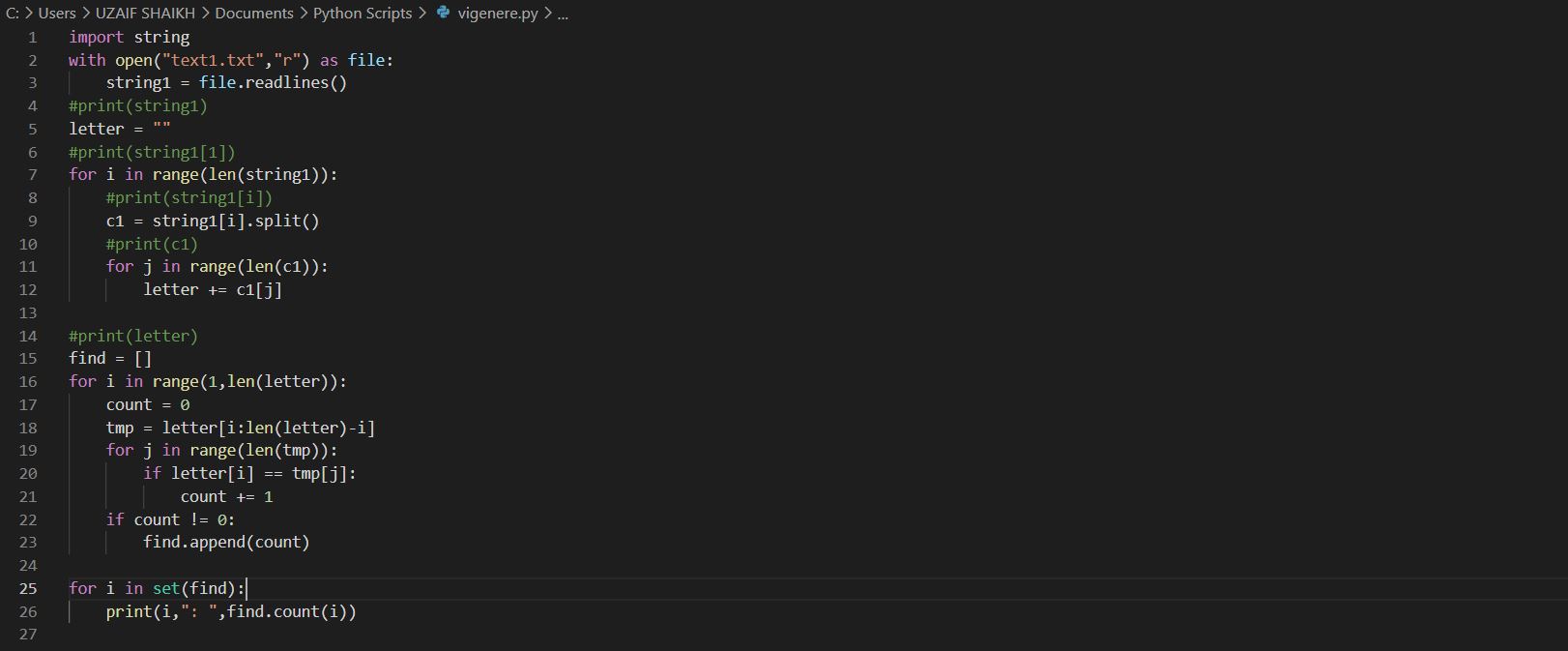


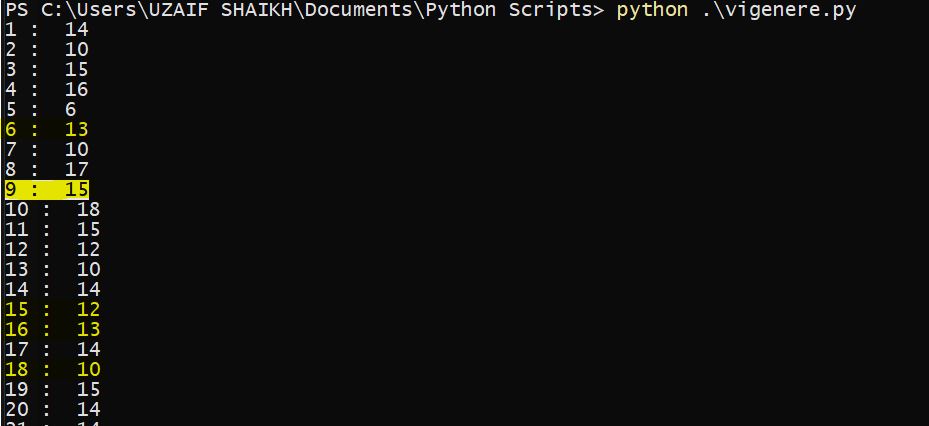
For Leve5, it was a poly-alphabetic cipher called Vigenère cipher so after doing some research on the cipher I got an idea on how to decrypt it, this video really helped full in understanding the cipher decryption trick ([**https://www.youtube.com/watch?v=LaWp\_Kq0cKs**](https://www.youtube.com/watch?v=LaWp_Kq0cKs) ), 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\_Kq0cKs**](https://www.youtube.com/watch?v=LaWp_Kq0cKs) ),  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.





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 ^ B = C and if A ^ 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.

