

## IIT Madras ONLINE DEGREE

## Programming in Python Professor. Sudarshan Iyengar Department of Computer Science & Engineering Indian Institute of Technology, Ropar Caesar Cipher

(Refer Slide Time: 0:16)

fasttableistooduponthehearthrugandpickedupthestickwhichourvisitorhadleftb Type 'copyright', 'credits' or ehindhimthenightbeforeitwasafinethickpieceofwoodbulbousheadedofthesortwhi information chisknownosapenanglowyerjustundertheheadwasabroadsilverbandnearlyaninchac | IPython 7.24.1 -- An enhanced Interactive Pythorosstojamesmortimermrcsfromhisfriendsofthecchwosengraveduponitmiththedate | Type '?' for help. ustsuchastickastheoldfashionedfamilypractitionerusedtocarrydignifie dsolidandreassurinawellwatsonwhatdovoumakeofitholmeswassittinawithhisback In [1]: ls youhaveeyesinthebackofyourheadihaveatleastamellpolishedsilverplatedcoffee phone\_large.txt sherlock.txt potinfrontofmesaidhebuttellmewatsonwhatdoyoumakeofourvisitorssticksincewe  $vebeen soun for tunate as to {\tt misshim} and {\tt have no notion} of {\tt hiserrand this} accidentals$ nirbecomesofimportanceletmehearyoureconstructthemanbyanexaminationof tithinksaidifollowingasfarasicouldthemethodsofmycompanionthatdrmortimeris asuccessfulelderlymedicalmanwellesteemedsincethosewhoknowhimgivehimthisma  $\circ$ koftheirappreciationgoodsaidholmesexcellentithinkalsothattheprobability  $sinfavour of his being a country practitioner {\tt who does a great deal of his visiting on formula} and {\tt otherwise} a$  ${\it cause this stick though or iginally avery hands ome one has been so knocked at the contract of the contra$ out that ican hardly imagine a town practitioner carrying it the thick iron ferrule is worn down so it is evident that he has done agree a tamount of wolking with it perfectly sounds. The content is the property of the pdsaid holmes and the nagain there is the friends of the cchi should guess that to be the same thing hunt the local hunt to whose members he has possibly given some surgical assistance.ance and which has made him as mall present at ion in return really wats on you excely our selfs aid holmes pushing back his chair and lighting acigar ettei ambound to say that in a constant of the constaIl the accounts which you have been sogood a stogive of myowns mall achievements you have habitually under rate dyour own abilities it may be that you are not your self luminous and the story of thebutyouareaconductoroflightsomepeoplewithoutpossessinggeniushavearemarkabl epowerofstimulatingiticonfessmydearfellowthatiamverymuchinyourdebthehadne ersaidasmuchbeforeandimustadmitthathiswordsgavemekeenpleasureforihadofte eenpiquedbyhisindifferencetomyadmirationandtotheattemptswhichihadm

If you remember, we did see a method called the Caesar Cipher. So, let us recollect what that was. Before that, let me take a look at the files in my current folder. I have stored a file called Sherlock dot txt. Let me open it on my editor. Sherlock dot txt we will open it. As you can see, this is Sherlock Holmes, The Hounds of Baskerville a wonderful story by Arthur Conan Doyle. You can read the story or even watch it. It is a wonderful piece. Anyways, that aside.

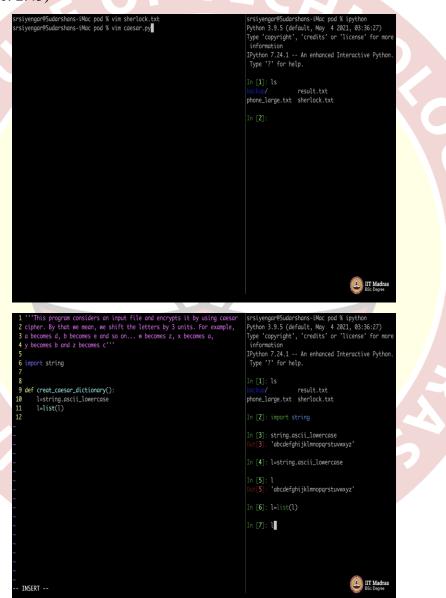
So, as you can see, I have removed all the unwanted characters, spaces and everything is in lowercase. I have even removed space. But still, you can make out what is being written here. Pick up the stick which our visitor had left behind him the night before it was a fine thick piece of wood. Of course, it is difficult to read, but with a lot of struggle you can indeed read it.

The point is now try to shift every single letter by 3 letters. By that I mean, your a should become a, b, c, a, b, c, d. And then your b should become, I am just using this to type, then b should become e and then c should become f, so on. How do you do that? I am going to create a dictionary and then convert this to every single letter should be shifted by 3 letters, c becomes d,

e, f, h becomes, h here, you see the second letter here, h becomes h, I, j, k, a becomes d, and so on. And I should put that onto a new file.

If you are wondering what we are saying in the earlier weeks we did try doing this on strings. Right now we will do it on a file. How do I do that? Let me go step by step. Let me write a code for this. First, let me come out of this file.

(Refer Slide Time: 2:45)

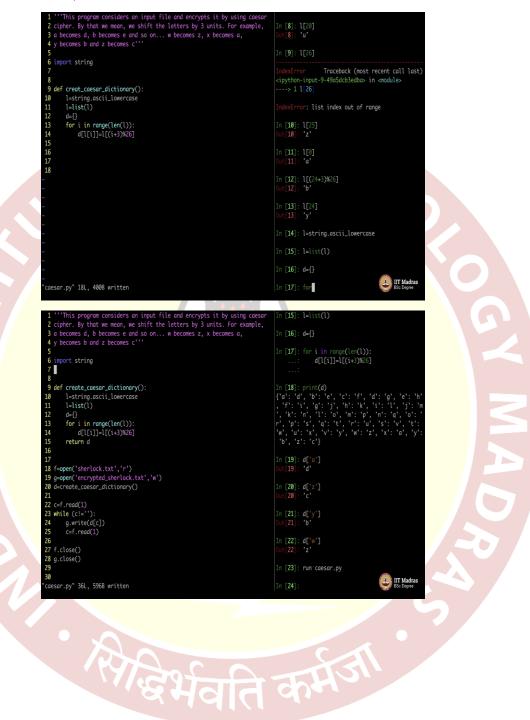


Vim caesar cipher caesar dot py, create a new file. Here, what do I do? This program considers an input file and encrypts it by using caesar cipher. By that we mean we shift the letters by 3 units. For example, a becomes d, b becomes e, and so on. If you are wondering what happens to z, z becomes, it rotates, z becomes let me write it, w becomes w, x, y, z and x becomes, y, z, a, y becomes b and z becomes c. Let me put this in next line so that it is easy for you people. And z becomes c.

So, this is the introduction. If you are still confused, go and look up what is caesar cipher. So, now what I will do is I will create a dictionary. Define, create, ceaser dictionary. What do you mean by that? By this, I mean, you will see in a minute what I am doing. There is something called import string. And what I will do here is I will create a list I which comprises of string dot ascii lowercase. Let me just see if that is there. Import string ascii lowercase comprises of all these things, very good.

So, and then I will once that is created, let us say, I equals string of ascii lowercase, I will be this. I will make it a list. It is very simple, I becomes list of I. So, that way, this becomes a word. It is always a good idea to type it on the right side and see on the interactive Python, what is happening and then code on the left side.

(Refer Slide Time: 5:47)



So, and then what I will do is you see your 1 of 20 will be, what am I doing, here, this side on the interactive Python, 1 of 20 is some u. L of 26 is nothing, because it ends at 25. L of 0 is a. So, now, whenever you do 1 of 24 plus 3, it becomes, it goes beyond 26. But then when you do mod 26, see what you will get? You will get b. L of 24 was y? Y is becoming b whenever you add plus 3 mod 26. So, that is the trick we are going to use now. Very simple.

So, what I will do is I will create a dictionary for i in range len of 1, d of 1 of i, which means 1 of 0, which is a, d of a will be equal to 1 of i plus 3 mod 26. So, this should do the trick right. Stare at this for a minute. So, I messed up big time. So, let me just spend a minute here in explaining what I have done.

So, you know what this does? It simply considers all ascii lowercase a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z, that is it. And then it converts that to a list here. And then I initialize a dictionary here. And that dictionary will have d of a should become c, d of a should become d, d of b should become e and so on. How do I do that? All I do is I iterate through the l. And then I explicitly state d of a is e. I shift that by three units, and so on and so forth. I do this modulo just so that I end up getting, for z I should get c, as you saw. If you are still confused, please look up what is caesar cipher or simply read what I have stated here.

So, now, what I will do is, I will try to see if this code indeed works fine. So, let us say I equals string of what was that, I equals list of I, d equals so much good, for i in a range, len of I, d of I of i is equal to I of i plus 3, I shifted by three units, modulo 26. Hopefully this works. Print d, so d

of a now will show you d and d of z as required is c. What is d of y, remember, should be b and so on, d of w is z, d of x is a.

So, I create this dictionary and I will return this dictionary just so that it can be used. Moment you say create ceaser, I got the spelling of create wrong here. I am a little particular about these things. Does not matter though. So, I create a dictionary like this. Now, what I do is I will go through every single file in the, every single letter in the file Sherlock dot txt. So, what do I do for that?

Let me write it in the main body of the file, f equals open Sherlock dot txt and then make it readable. I will open another file, call it encrypted Sherlock dot txt. It should be write. And all I do is I will read one character at a time from my file f. And while this character is not equal to end of the file, correct remember this, it is not the end of the file, then what I do, what do I do, let me think.

So, I will be writing this, not this character, but d of that character, so I will write d of this character to the new file encrypted dot Sherlock dot txt, that is all, as simple as this. Once this is done, what happens here? This keeps getting returned. And then what I do is again, I said c equals f read 1. Why do I do that? It is very simple.

Let me illustrate that. I do this part. This part here writes to my new file. What is this part do? This part simply reads the next character, pretty simple. Next character, in which file, in this file, because it is f read, as you can see. It is f read. I believe you are familiar with what I am stating. So, that is pretty much it. And at the end, I will close my file f. I will close my file g.

Let me quickly go through the entire thing. So, I am saying, there is a small mistake here. You see, I am saying d of c, what is d of c. You must create d, d is the dictionary that you create, which is dictionary, that it. Then d gets created. Automatically d of a will be, d of b will be e and so on, d of z will be c and so on. I created, very good.

And then I will start reading from the file f, I am reading the first letter, and then while it is not reaching the end, whenever I read from a file, if it is reaches the end, then it will assign null space which is colon, colon, nothing in between If c is not that then I go ahead and write that to a new file, encrypted dot Sherlock, which is g. I open it as g. g dot write you have see, and then I go to the next letter in the file f.

And again, while keeps repeating. It stops when it reaches the end of the file, as simple as that. And then I close these two files, which means my Sherlock encrypted, encrypted Sherlock dot txt should have the encrypted version of the file. Let me try running this, say this come out of this and then run caesar dot py. It got executed without any errors.

Let me open. This is how you open my file or I will open from the directory, so eod, open encrypted Sherlock. You see, Sherlock dot txt is 246 kb, encrypted Sherlock is also 246 kb, because it is letter by letter. See, everything is encrypted here. Is not it awesome? You wrote a piece of code to encrypt a letter, I am just zooming in so that you can see it.

(Refer Slide Time: 14:19)

Let me go f, k, d. F means what? F means b, c, d, e, f, c. C is becoming f, h is becoming probably h, i, j, k. H is becoming k. A is becoming d. This was actually chapter. The first word was chapter in the original file. Let us see Sherlock dot txt, chapter in the original file. It is getting encrypted and the entire thing gets encrypted. It is a big file.

Nobody can make any sense out of it unless you decrypt it. How do you decrypt it? You should probably create another dictionary, which will do the subtraction of three letters the other side, opposite side. I am not going in detail because I have a feeling you have gained the maturity by now. You know what is what. Or maybe if you are not, then go through it once again.

Again, this code as I am typing, you cannot really keep up with my pace, maybe you should pause and then write the code, ensure that there are no errors anywhere and then execute it. So,

what you can do is this is for creating encrypted Sherlock dot txt, but what if you give this as an input, you should be able to, let me write this here, try writing a code which takes the encrypted Sherlock dot txt as an input file and decrypts it and gets back your Sherlock dot txt. This will be your homework. Try doing it.

Now, this does not stop here. We are going to get into more sophisticated what is called the crypt analysis. I will not talk in detail right now. In the next week we will see that. But as of this week, this code on this tech should be more than enough. Go through it, understand what I have done and get familiarized with file handling.

