Substitution Cipher

The science of secrecy 03

So let us try to code substitution cipher here, for substitution cipher we have an input file here named ip underscore file, it has some text i need to convert this text in such a way so that it is not recognise by the third person for that i will be using substitution cipher so for that i need a string of alphabets in which i can substitute the letters, python provide with the string named string dot ascii underscore letters i will print it so i will write print string dot ascii underscore letters as you can see we have the letters in lower case as well as in the upper case so i will be substituting this string in such a way so that it is not recognise the text present in our input file is not recognise by the third person i will be using this particular string for that so in order to execute the substitution part i will write import string after that i will initialise a dictionary called dict, i hope that you are already familiar with dictionaries, strings as well as file handlings because will be using all three of them in this particular programme and if you are not familiar with these concepts i would suggest you to go though the previous videos, please go through the previous videos and then watch this programming screen cast. Now we have dictionary named dict is equal to dict is equal to curly braces this is how we initialise a dictionary, for converting this particular string to a substituted format i will write for i in range length string dot ascii underscore letters. In this particular dictionary if any letter is at ith position i will be substituting it by i minus one position, position letter it's your choice by with which letter you want to substitute a particular letter here if i am substituting a letter given letter by its them by the previous letter so we will have here, A will be substituted by Z, B would be substituted by A, C would be substituted by B, B would be substituted by C. This is how our dictionary is going to work, so i will write string dot ascii letters, string dot ascii underscore letters at ith position will be substituted by string dot ascii underscore letters at i minus one position here i used minus one you can even use plus one, plus two, even minus two minus three it's your wish i am substituting it my minus oneth letter so that you can tip your get idea of how our programming is working, it would be easy to observe this particular dictionary so i will just print dictionary here so that so you can get the idea of what is happening over here. So here we have the dictionary as you can see capital z is A substituted by capital Z, B is substituted by A, C is substituted by B, D is substituted by C this is how our substitution is working, so we have all the substitution in this particular dictionary named dict, now we will use this dictionary dict to convert our input file. For that first of all we need to open our input file named ip underscore file so i will write with open ip underscore file dot txt as f then i will write while true i need to read this file by character by character and i need to substitute a particular character according to the dictionary so i will take a variable here named C, C is equal to f dot read now i need to check one or two things here first of all i will be checking whether we have encounter end of file or not, for that i will write if not c, if the if the file pointer hasn't encounter any character that means it has reached end of file, so in this particular case we will print end of file and it will break out of this file loop and if c if the file pointer has encounter a c which is already present in the dictionary, if C in dict in that

particular case i will take a string here name data, please initialise the string data here, how can you do that? You can initialise through double quotes so we have initialise our string data, data is equal to dict of C, if C is present in dictionary in that particular case data will be equal to dict of C and if C is not present in the dictionary then we can't do anything will just write data is equal to C instead of dict of C, please note the fact that in our dictionary dict only alphabets are present, in lower case as well as upper case and if in our file some if in our file some integers zero to nine or some special symbols are present that will not be substituted so here is an exercise for you, if you encounter a file with some special symbols and integers how can you apply substitution factor on that particular file its an exercise to you, its left to you how can you do that? So here we have the string data which has the substituted file, which has a substituted data so i will just print it. I will just write print data let us try to print this. So now we have the data, but the data is exactly like the input file so there is some error in our programme, here if we are reading the file we need to supply a bullion value here so i will just supply one and try to read it here we have the substituted file so here is the mistake, when we are reading the file when we need to supply some bullion value here one here. So as you can see that it has substituted our input file and this is something we can't read and we can't recognise ok so what will i do here is, i will store this output in a file, you can get a clear cut idea of the substitution happening over here so i will take another file here named file is equal to open op underscore file dot txt and i will open this file in writing mode since we need to write it, and what next we need to do here is i need to write this particular string data in our file so i will just write here file dot write under curly braces we will write data ok after we are done with the writing part i will close this file i will write file dot close round braces so now let us try to run this programme again so here we have the substitute text let us open the file output file or op underscore op underscore file as you can see here we have the data in the substituted form this is something we can't recognise we can't figure out that this text was actually this and we have substituted it by using substitution cipher so now we are done with the programme, i will go through the program again. First of all there is a string present in python name string dot ascii underscore letters we use this string for the substitution part here we are substituting the letters present in the string by i minus oneth letter, here we have for that we are using dictionary we have initialise the dictionary here in dict after that we are executing the substitution part in this particular part we are writing dict string dot ascii underscore letters at ith position will be substituted by i minus oneth letter this is how we are doing the substitution please note that dict dictionary has dictionaries have keys and value in this particular dictionary keys are the letters present in the string and the values are the substitute letters i repeat keys are the values present in the string and values are the substitute letters, after that we are opening our file our input file and we are reading a character by character for that we need to supply a bullion variable here one as to read the file character by character then we are checking some conditions here first condition we are checking here is whether we have encounter the end of file or not, if we have encountered end of file in that particular case our programme will print end of file and it will break out of this loop and we are checking if the particular character present in the input file is actually present in our dictionary, if it is not present then it will then it will only write this C in data otherwise if it is present it will write dict of C the substituted letter in the data. At the end we are writing this string data in output in an output file so that we can get the clear cut idea of

how the substitution is working and then we are printing the data and finally we are closing the file. So as you can see here we have two files here this is the output file and this is the input file, here the in input file you can read the text but in output file the output file is converted to some other text using the substitution cipher which is not recognised which can't be recognised by the third person until and unless he gets to know that the substitution cipher is used here so this is how you quote for substitution cipher and convert many more text, i hope this programming screen cast was useful to you guys. Happy learning.