

ESCUELA COLOMBIANA DE INGENIERIA JULIO GARAVITO

IT SECURITY AND PRIVACY GRUPO 1L

CRACKING PRACTICE LABORATORY 7

SUBMITTED BY: JUAN PABLO FERNANDEZ GONZALES MARIA VALENTINA TORRES MONSALVE

SUBMITTED TO: Ing. DANIEL ESTEBAN VELA LOPEZ

BOGOTÁ D.C.

DATE: 10/03/2025

Breaking the Shift Cipher



This objective is writing a Python script that contains the encrypt and decrypt functions for the shift cypher, as well as a brute force function, and use it to encrypt the following texts using the provided key.

Program Development:

The **getIndex**(**abc**, **letter**) function takes an alphabet sequence (abc) and a letter (letter) as input. Its purpose is to find the position of the letter within the given alphabet and return its index. This is essential for determining the current location of a character before applying the shift cipher.

The **getLetter**(**abc**, **index**) function takes an alphabet sequence (abc) and an index (index) as input. Its function is to return the letter found at the specified position within the alphabet. This allows retrieving the new encrypted character after performing the shift.

The **enc(k, abc, str)** function implements message encryption using the shift cipher. It takes three parameters: k, which represents the number of positions to shift; abc, the alphabet used; and str, the plaintext message to be encrypted. For each letter in the message, the function retrieves its index using getIndex(), calculates the new position by adding kand applying the modulus operation ((index_act + k) % 26), and obtains the new letter with getLetter(). Finally, it constructs and returns the encrypted message.

We will be testing with the following exercises:

1. ADVANCEDCRYPTOSYSTEMSAREPOWERFUL, with key 8.

Result: ILDIVKMLKZGXBWAGABMUAIZMXWEMZNCT

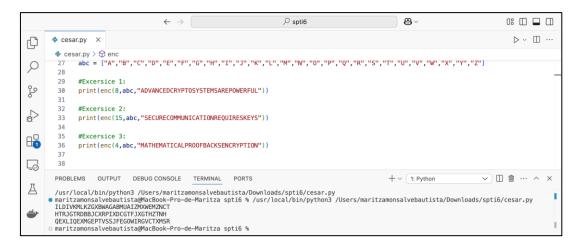
2. SECURECOMMUNICATIONREQUIRESKEYS, with key 15.

Result: HTRJGTRDBBJCXRPIXDCGTFJXGTHZTNH

3. MATHEMATICALPROOFBACKSENCRYPTION, with key 4.



Result: QEXLIQEXMGEPTVSSJFEGOWIRGVCTXMSR



This objective is writing a Python script that contains the encrypt and decrypt functions for the shift cypher, as well as a brute force function, and use it to decrypt the following texts using brute force.

Program Development:

The **getIndex(abc, letter)** function takes an alphabet (abc) and a letter (letter) as input. Its purpose is to find the position of the letter within the given alphabet and return its index. This function is essential for determining the current location of a character before performing encryption or decryption operations.

The **getLetter(abc, index)** function takes an alphabet (abc) and an index (index) as input. Its function is to return the letter found at the specified position within the alphabet. This allows retrieving the correct character after performing a shift operation in encryption or decryption.

The **dec(k, abc, str)** function implements the decryption process of the Shift Cipher. It takes three parameters: k, which represents the number of positions to shift in reverse; abc, the alphabet used; and str, the encrypted message. For each letter in the message, the function retrieves its index using getIndex(), calculates the new position by subtracting kand applying the modulus operation ((index_act - k) % 26), and obtains the original letter using getLetter(). Finally, it constructs and returns the decrypted message.

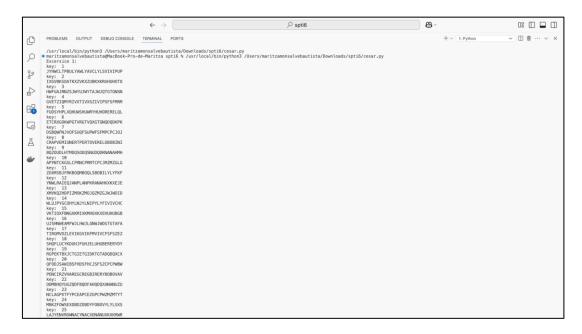
The **brute_force(abc, str)** function attempts to decrypt a message without knowing the key (k). To achieve this, it iterates through all possible values of k (from 1 to 25) and applies the dec() function with each one, displaying the results. This allows identifying the correct key by observing which result makes sense in the language the message was originally encrypted in.



```
08 🗆 🗆 🗆
                                                                                                                                                                83
             cesar.py ×
P
P
                          def getIndex(abc , letter):
    return abc.index(letter)
Şo
                          def getLetter(abc, index):
                                   return abc[index]
                         def enc(k,abc, str):
    response = ""
    for i in range(len(str)):
        index_act = getIndex(abc,str[i])
        new_index = (index_act + k) % 26
        response += getLetter(abc,new_index)
    return response
\mathrel{<_{\tilde{\Xi}}}
Д
                         def dec(k,abc,str):
                                 response = getIndex(abc,str[i])
new_index = (index_act - k) % 26
response += getLetter(abc,new_index)
return response
—
                          def brute_force(abc,str):
```

We will be testing with the following exercises:

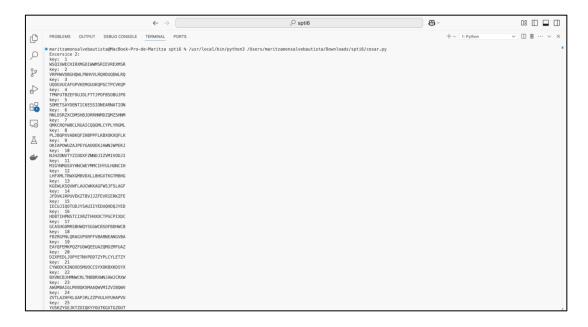
1. KZIXDMUQCVMZBXMZBWDMZMTWJWJQVQ



El resultado con más coherencia en inglés es la 8.

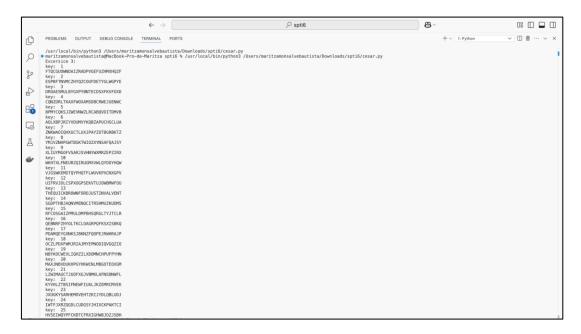
2. XTRJYXFDIJSYNHPJXXNTSJFWSFYNTS





El resultado con más coherencia en inglés es la 5.

3. GURDHVPXOEBJASBEQWHFGVAINYIRAG



El resultado con más coherencia en inglés es la 13.

The objective of the exercise is to implement and understand a substitution cipher that allows both encryption and decryption of messages by swapping two alphabets.



The enc function performs a substitution cipher where abc represents the original characters, key the encrypted characters, and str the text to transform. It iterates through abc, replacing each letter with its corresponding one in key(in lowercase) and returns the result in uppercase. By swapping abc and key, the same function can decrypt the text. For example:

with abc="ABCDEFGHIJKLMNOPQRSTUVWXYZ" and key="QWERTYUIOPA SDFGHJKLZXCVBNM", encrypting "HELLO WORLD" gives "ITSSG VGKSR", and decrypting "ITSSG VGKSR" returns "HELLO WORLD", proving the function is bidirectional.



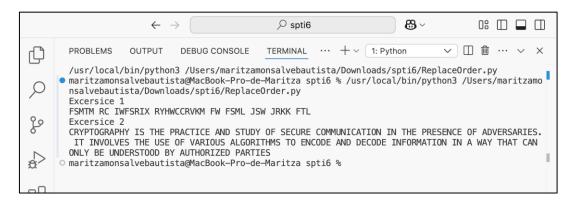
- Text: THERE IS NOTHING IMPOSSIBLE TO THEY WHO WILL TRY
- Key: BVZPMEXSRUAKYIWHOTCFDNJQLG

Result: FSMTM RC IWFSRIX RYHWCCRVKM FW FSML JSW JRKK FTL

- Ciphertext: SEFKWLREHKIF MC WIV KEHSWMSV HTZ CWDZF LY CVSDEV SLOODTMSHWMLT MT WIV KEVCVTSV LY HZQVECHEMVC. MWMTQLAQVC WIV DCV LY QHEMLDC HARLEMWIOC WL VTSLZV HTZ ZVSLZV MTYLEOHWMLT MT H NHF WIHW SHT LTAF JV DTZVECWLLZ JF HDWILEMPVZ KHEWMVC.
- Key: HJSZVYRIMUBAOTLKXECWDQNGF

Result: CRYPTOGRAPHY IS THE PRACTICE AND STUDY OF SECURE COMMUNICATION IN THE PRESENCE OF ADVERSARIES. IT INVOLVES THE USE OF VARIOUS ALGORITHMS TO ENCODE AND DECODE INFORMATION IN A WAY THAT CAN ONLY BE UNDERSTOOD BY AUTHORIZED PARTIES





The objective of this exercise is to develop a program that analyzes the frequency of characters in a given ciphertext and replaces the most common ones based on the standard English letter frequency table. This will help in understanding frequency analysis as a cryptographic technique and how it can be used to decrypt substitution ciphers. Additionally, the program will allow for manual adjustments, reinforcing the process of cryptanalysis and improving decryption accuracy.

The *frequency*(*alphabet*, *text*) function calculates the frequency of each letter in the given text. It iterates through each letter of the alphabet, counts its occurrences in the text, and stores the results as a list of pairs [letter, count]. This helps analyze the distribution of characters in the encrypted text.

The *order_frequency*(*repetitions*) function takes the frequency list generated by the previous function and sorts it in descending order based on the number of occurrences of each letter. This helps identify the most common characters in the text, which is useful for frequency-based decryption techniques.

The *replace_frequency(history_frequencies, text, frequencies)* function automatically replaces the five most frequent letters in the text with the five most common letters in English: E, T, A, O, I. It takes the most repeated letters in the text and substitutes them with the corresponding letters from the history_frequencies list. This is a first step in decrypting the message using frequency analysis.

The *replace_user(text, frequencies)* function allows the user to manually replace the remaining letters in the text. Starting from the sixth most frequent letter, the program asks the user which letter they want to replace it with, displaying the available options. It then updates the text with the changes and continues until all letters have been substituted.



Finally, the *replace_error(text)* function offers the possibility of making additional modifications to the processed text. It asks the user if they want to change any letter, and if they do, it allows them to input the letter to be modified and its replacement. This process repeats until the user decides to stop making changes, ensuring a refined decryption of the message.

By frecuency we replace G, C, S, H y R for e, t, a, o and the i. Respectively.

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

//usr/local/bin/python3 /Users/maritzamonsalvebautista/Downloads/spti6/frecuencias.py
//usr/local/bin/python3 /Users/maritzamonsalvebautista/Downloads/spti6/frecuencias.py
| /usr/local/bin/python3 /Users/maritzamonsalvebautista/Downloads/spti6/frecuencias.py
|
```

Then, we start to replace it trying to obtain some frase that make sense. Even if it was complicated, after the replacement we obtain the following text:

"t lmng oske tgm, sn t gtltxy fta, fta twty... so si t dtaq oske fma ohe aebellsmn. tlohmugh ohe detoh iota hti been deioamyed, skdeastl oammdi htve dasven ohe aebel fmacei famk ohesa hsdden btie tnd duaiued ohek tcamii ohe gtltxy. evtdsng ohe daetded skdeastl iotafleeo, t gamud mf faeedmk fsghoeai led by luqe iqywtlqea hti eiotblsihed t new iecaeo btie mn ohe aekmoe sce wmald mf hmoh. ohe evsl lmad

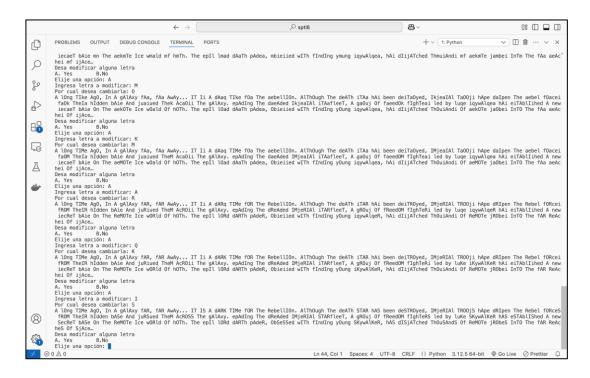


dtaoh vtdea, mbieiied wsoh fsndsng ymung iqywtlqea, hti dsidtoched ohmuitndi mf aekmoe dambei snom ohe fta aetchei mf idtce..."

Then we are going to replace until we have something that make sense:

"A lOng TIMe AgO, In A gAlAxy fAR, fAR AwAy... IT IS A dARK TIMe fOR The Rebellion. Although The deAth Star has been deStroyed, IMPerial Troops have driven the Rebel forces from their hidden base and Pursued them across the galaxy. eVading the dreaded IMPerial Starfleet, a group of freedom fighters led by luke skywalker has established a new Secret base on the remote ice world of hoth. The eVil lord darth vader, obsessed with finding young skywalker, has dispatched thousands of remote probes into the far reaches of space..."

Where the capital letters were replaced again. Where the .



IT SECURITY AND PRIVACY



