

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO



FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

DISEÑO Y ANÁLISIS DE ALGORITMOS

PROYECTO

DESCIFRAR TEXTO DE CIFRADO POR SUSTITUCIÓN

EQUIPO 17:

MANZANO PONCE JOSUÉ OLVERA MARTÍNEZ LEONARDO ORTEGA BATÚN LUIS FERNANDO

PROFESOR:
PEREZ MEDEL MARCELO

GRUPO: 1507

FECHA: 23 DE NOVIEMBRE DEL 2023

SEMESTRE 2024-I

TEXTO 1:

Texto cifrado:

Oitlt xlt onb ovjtc bd jtbjqt nib ngqq otqq vbr oixo vbr zxmmbo yxkt x egddtltmzt gm oigc nblqe: oibct nib xlt xdlxge ob olv xme oibct nib xlt xdlxge vbr ngqq crzztte Crzztcc gc qgkgmu vbrlctqd, qgkgmu nixo vbr eb, xme qgkgmu ibn vbr eb go Nitmtftl vbr dgme vbrlctqd bm oit cget bd oit yxwblgov, go gc ogyt ob jxrct xme ltdqtzo Kttj vbrl dxzt xqnxvc obnxle oit crmcigmt xme cixebnc ngqq dxqq htigme vbr Gd vbr ixft tftlvoigmu rmetl zbmolbq, vbr xlt mbo ybfgmu dxco tmbrui Go gc erlgmu brl exlktco ybytmoc oixo nt yrco dbzrc ob ctt oit qguio

(idioma detectado: Ingles)

Código:

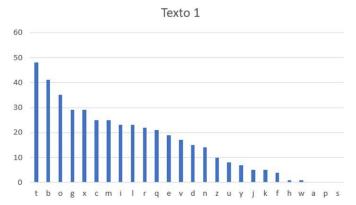
```
21 def cargaPalabras():
      archivo = open(os.path.join(ruta_carpeta, 'Ingles', 'ingles_diccionario.txt'), 'r')
      renglon = archivo.readline()
24
      palabras = renglon.split()
25
      print (len(palabras), 'palabras leidas')
      return palabras
28 # Abre el archivo donde viene el texto cifrado
29 def cargaCifrado():
      archivo = open(os.path.join(ruta_carpeta, 'Texto1.txt'), 'r')
      renglon = archivo.readline()
      return renglon
34 def descifraSustituye(cadena, alfabetoLlave):
      cadena = cadena.lower()
      alfabeto = 'abcdefghijklmnopqrstuvwxyz'
      nuevaCadena = ""
       for letra in cadena: # recorre texto
38
           if letra in alfabeto: # busca la letra en el alfabeto
40
               posicion = alfabeto.find(letra) # obtiene posicion del alfabeto
              nuevaCadena = nuevaCadena + alfabetoLlave[posicion] # pos nuevo alf
41
42
              nuevaCadena = nuevaCadena + letra # si no esta en alfabeto
43
44
       return nuevaCadena
45
46 dic = cargaPalabras()
47 cifrado = cargaCifrado()
```

La primera función (cargaPalabras) abre el documento en donde guardamos nuestro diccionario de inglés y almacena estas palabras en una variable. La segunda función (cargaCifrado) obtiene el contenido del txt "Texto 1" en donde almacenamos nuestro primer texto cifrado. La última función (descifraSustituye) toma una cadena, que será nuestro texto a descifrar, y una llave, la cual hay que encontrar, y recorrerá la cadena caracter por

caracter obteniendo la posición de este en el alfabeto normal y sustituyendola por la posición en nuestra llave.

La salida del histograma del Texto cifrado 1, es el siguiente:

{'a': 0, 'b': 41, 'c': 25, 'd': 15, 'e': 19, 'f': 4, 'g': 29, 'h': 1, 'i': 23, 'j': 5, 'k': 5, 'l': 23, 'm': 25, 'n': 14, 'o': 35, 'p': 0, 'q': 21, 'r': 22, 's': 0, 't': 48, 'u': 8, 'v': 17, 'w': 1, 'x': 29, 'y': 7, 'z': 10}



En el histograma de frecuencias podemos ver que las letras que más se repiten son t, b, o, g lo que nos puede servir para la búsqueda del alfabeto, ya que será imposible encontrarles un valor, así que en nuestra llave la sustituiremos por una X.

posA="abcdefghilmnopgrstuvz" posB="abcdefghilmnopgrstuvz" posC="abcdefghilmnopqrstuvz" posD="abcdefghilmnopgrstuvz" posE="abcdefghilmnopqrstuvz" posF="abcdefghilmnopgrstuvz" posG="abcdefghilmnopgrstuvz" posH="abcdefghilmnopqrstuvz" posJ="abcdefghilmnopgrstuvz" posK="abcdefghilmnopqrstuvz" posL="abcdefghilmnopgrstuvz" posM="abcdefghilmnopgrstuvz" posN="abcdefghilmnopqrstuvz" posO="abcdefghilmnopqrstuvz" posP="abcdefghilmnopqrstuvz" posQ="abcdefghilmnopgrstuvz" posR="abcdefghilmnopqrstuvz" posU="abcdefghilmnopgrstuvz" posV="abcdefghilmnopgrstuvz" posW="abcdefghilmnopqrstuvz" posZ="abcdefghilmnopgrstuvz"

Empezando a descifrar por sustitución:

El problema al cual nos enfrentamos, si quisiéramos resolverlo por fuerza bruta, sería de un orden n! lo cual representa un gran problema, así que para evitar tardar milenios en resolverlo, haremos una sustitución buscando las palabras que se puedan parecer que tengamos en nuestro diccionario, eliminando posibles letras del alfabeto hasta dar con su valor real (convirtiendo un problema np a p).

Lo que haremos será intentar buscar alguna palabra que tenga alguna característica en particular, letras que se repitan, una longitud determinada; sin combinamos estos dos elementos y buscamos dentro de nuestra amplia gama de palabras en el diccionario alguna que se acople con nuestras necesidades podremos encontrar algunas palabras candidatas para nuestra palabra cifrada. Si encontramos varias palabras podemos suponer que los primeros caracteres de nuestras palabras encontradas en el diccionario son buenos candidatos para el posible carácter cifrado, esto debemos hacerlo con cada carácter de la palabra descifrada, en caso de solo encontrar una palabra es más que excelente, ya los caracteres de esta palabra son los valores reales de los caracteres de nuestra palabra cifrada.

Esto hay que tomarlo en cuenta ya que hay que estar actualizando constantemente los valores de nuestros posibles caracteres, es posible que con la primer palabra obtengamos muchas palabras como candidatos, pero si continuamos actualizando los valores de nuestros posibles caracteres y volvemos a probar esta primer palabra, puede que nos de menos palabras de las que nos dio en un principio.

Esto hay que hacerlo constantemente y es probable que tengamos problemas, ya que hay una posibilidad que una palabra cifrada no se encuentre en nuestro diccionario, supongamos que una palabra hay dos palabras candidatas, solo una es la real, pero esa no se encuentra en nuestro diccionario, es entonces que nuestro código nos muestra solo una palabra y nos podemos quedar con la idea que esa palabra es la real, cuando no es así, esto es una situación complicada ya que podemos quedarnos un valor erróneo en un posible carácter y a medida que avancemos en nuestro código tendremos problemas para encontrar posibles palabras candidatas. Podemos resolver estos problemas o darnos cuenta dónde está el error intercambiando los caracteres que hemos descubierto en las palabras que están cifradas y el resultado meterlo en un traductor, en caso que el traductor no pueda identificar la palabra, es porque algún carácter tiene algún error.

Como se muestra a continuación, este fue el proceso que seguimos para descifrar el primer texto y básicamente es el mismo procedimiento que se explicó anteriormente, esto para ambos textos cifrados, el primero y el segundo.

```
50 posA = 'abcdefghijklmnopqrstuvwxyz' # 0
51 posB = 'abcdefghijklmnopqrstuvwxyz'
52 posC = 'abcdefghijklmnopqrstuvwxyz'
53 posD = 'abcdefghijklmnopqrstuvwxyz'
54 posE = 'abcdefghijklmnopqrstuvwxyz'
55 posF = 'abcdefghijklmnopqrstuvwxyz'
56 posG = 'abcdefghijklmnopqrstuvwxyz'
57 posH = 'abcdefghijklmnopqrstuvwxyz'
58 posI = 'abcdefghijklmnopqrstuvwxyz'
59 posJ = 'abcdefghijklmnopqrstuvwxyz'
60 posK = 'abcdefghijklmnopqrstuvwxyz'
61 posL = 'abcdefghijklmnopqrstuvwxyz'
62 posM = 'abcdefghijklmnopqrstuvwxyz'
63 posN = 'abcdefghijklmnopqrstuvwxyz'
64 pos0 = 'abcdefghijklmnopqrstuvwxyz'
65 posP = 'abcdefghijklmnopqrstuvwxyz' # 0
66 posQ = 'abcdefghijklmnopqrstuvwxyz'
67 posR = 'abcdefghijklmnopqrstuvwxyz'
68 posS = 'abcdefghijklmnopqrstuvwxyz' # 0
69 posT = 'abcdefghijklmnopqrstuvwxyz'
70 posU = 'abcdefghijklmnopqrstuvwxyz'
71 posV = 'abcdefghijklmnopqrstuvwxyz'
72 posW = 'abcdefghijklmnopgrstuvwxyz'
73 posX = 'abcdefghijklmnopqrstuvwxyz'
74 posY = 'abcdefghijklmnopqrstuvwxyz'
75 posZ = 'abcdefghijklmnopqrstuvwxyz'
76 c = 0
77
78 #probando con Crzztcc
79 for p in dic:
80
       if len(p) == 7:
81
           if p[0] == p[5] and p[0] == p[6] and p[2] == p[3]:
82
83
               print(p)
84 print(c)
```

```
Drive already mounted at /content/drive;
55900 palabras leidas
success
1
```

Probando con: egddtltmzt

```
88 posA = 'abcdefghijklmnopqrstuvwxyz'
89 posB = 'abcdefghijklmnopqrstuvwxyz'
 90 posC = 's'
 91 posD = 'abcdefghijklmnopqrstuvwxyz'
92 posE = 'abcdefghijklmnopqrstuvwxyz'
 93 posF = 'abcdefghijklmnopqrstuvwxyz'
 94 posG = 'abcdefghijklmnopgrstuvwxyz'
 95 posH = 'abcdefghijklmnopqrstuvwxyz'
 96 posI = 'abcdefghijklmnopqrstuvwxyz'
97 posJ = 'abcdefghijklmnopqrstuvwxyz'
 98 posK = 'abcdefghijklmnopqrstuvwxyz'
99 post = 'abcdefghijklmnopqrstuvwxyz'
100 posM = 'abcdefghijklmnopqrstuvwxyz'
101 posN = 'abcdefghijklmnopqrstuvwxyz'
102 posO = 'abcdefghijklmnopqrstuvwxyz'
103 posP = 'abcdefghijklmnopqrstuvwxyz'
104 posQ = 'abcdefghijklmnopqrstuvwxyz'
105 posR = 'u'
106 posS = 'abcdefghijklmnopqrstuvwxyz'
107 posT = 'e'
108 posU = 'abcdefghijklmnopqrstuvwxyz'
109 posV = 'abcdefghijklmnopqrstuvwxyz'
110 posW = 'abcdefghijklmnopqrstuvwxyz'
111 posX = 'abcdefghijklmnopqrstuvwxyz'
112 posY = 'abcdefghijklmnopqrstuvwxyz'
113 posZ = 'c'
114 c = 0
115
116 # probando con egddtltmzt
117 for p in dic:
118
       if len(p) == 10:
119
            if p[2] == p[3] and p[4] in posT and p[4] == p[6] and p[4] == p[9]:
120
                c = c + 1
121
                print(p)
122 print(c)
```

```
Drive already mounted at /content/drive;
55900 palabras leidas
difference
1
```

Probando con: zbmolbq

```
126 posA = 'abhijklmopqtvwxyz'
127 posB = 'abhijklmopqtvwxyz'
128 posC = 's'
129 posD = 'f'
130 posE = 'd'
131 posF = 'abhijklmopqtvwxyz'
132 posG = 'abhijklmopqtvwxyz'
133 posH = 'abhijklmopqtvwxyz'
134 posI = 'g' #error
135 posJ = 'abhijklmopqtvwxyz'
136 posK = 'abhijklmopqtvwxyz'
137 posL = 'r'
138 posM = 'n'
139 posN = 'abhijklmopqtvwxyz'
140 posO = 'abhijklmopqtvwxyz'
141 posP = 'abhijklmopqtvwxyz'
142 posQ = 'abhijklmopqtvwxyz'
143 posR = 'u'
144 posS = 'abhijklmopqtvwxyz'
145 posT = 'e'
146 posU = 'abhijklmopqtvwxyz'
147 posV = 'abhijklmopqtvwxyz'
148 posW = 'abhijklmopqtvwxyz'
149 posX = 'abhijklmopqtvwxyz'
150 posY = 'abhijklmopqtvwxyz'
151 posZ = 'c'
152 c = 0
153
154 # funcion para definir nuesto nuevo alfabeto quitando los caracteres encontrados
155 nuevoAlfabeto = 'abcdefghijklmnopqrstuvwxyz'
156 caracteresEncontrados = ['s', 'f', 'd', 'g', 'r', 'n', 'u', 'e', 'c']
157 for a in caracteresEncontrados:
158 | nuevoAlfabeto = nuevoAlfabeto.replace(a, "")
159 print (nuevoAlfabeto)
160
161 # probando en zbmolbq
162 for p in dic:
        if len(p) == 7:
            if (p[0] in posZ and p[1] in posB and p[2] in posM and p[3] in posO
164
165
                and p[4] in posL and p[1] == p[5] and p[6] in posQ):
                 c = c + 1
166
167
               print(p)
168 print(c)
169 # Nos da 4 resultados asi que usamos el abecedario reducido
170 # Al usar los abecedarios reducidos obtenemos un resultado: control
```

```
Drive already mounted at 55900 palabras leidas abhijklmopqtvwxyz control
```

Probando con: ybytmoc

```
173 posA = 'abhijkmpqvwxyz'
174 posB = 'o'
175 posC = 's'
176 posD = 'f'
177 posE = 'd'
178 posF = 'abhijkmpqvwxyz'
179 posG = 'abhijkmpqvwxyz'
180 posH = 'abhijkmpqvwxyz'
181 posI = 'g'
182 posJ = 'abhijkmpqvwxyz'
183 posK = 'abhijkmpqvwxyz'
184 posL = 'r'
185 posM = 'n'
186 posN = 'abhijkmpqvwxyz'
187 pos0 = 't'
188 posP = 'abhijkmpqvwxyz'
189 posQ = '1'
190 posR = 'u'
191 posS = 'abhijkmpqvwxyz'
192 posT = 'e'
193 posU = 'abhijkmpqvwxyz'
194 posV = 'abhijkmpqvwxyz'
195 posW = 'abhijkmpqvwxyz'
196 posX = 'abhijkmpqvwxyz
197 posY = 'abhijkmpqvwxyz'
198 posZ = 'c'
199 c = 0
200
201 # funcion para definir nuesto nuevo alfabeto quitando los caracteres encontrados
202 nuevoAlfabeto = 'abcdefghijklmnopqrstuvwxyz'
203 caracteresEncontrados = ['o','s','f','d','g','r','n','t','l','u','e','c']
204 for a in caracteresEncontrados:
205 | nuevoAlfabeto = nuevoAlfabeto.replace(a, "")
206 print (nuevoAlfabeto) # abhijkmpqvwxyz
207
208 # probando en ybytmoc
209 for p in dic:
210 | if len(p) == 7:
211
             if (p[0] \text{ in posY and } p[1] \text{ in posB and } p[2] == p[0] \text{ and } p[3] \text{ in posT}
                and p[4] in posM and p[5] in posO and p[6] in posC):
212
213
                 c = c + 1
214
                 print(p)
215 print(c)
216 # 1 resultado : moments
```

```
Drive already mounted at /content/drive;
55900 palabras leidas
abhijkmpqvwxyz
moments
1
```

```
219 posA = 'abhijkpqvwxyz'
220 posB = 'o'
221 posC = 's'
222 posD = 'f'
222 posb = 'd'
224 posF = 'abhijkpqvwxyz'
225 posG = 'abhijkpqvwxyz'
226 posH = 'abhijkpqvwxyz'
227 posI = 'g'
228 posJ = 'abhijkpqvwxyz'
229 posK = 'abhijkpqvwxyz'
230 posL = 'r'
231 posM = 'n'
232 posN = 'abhijkpqvwxyz'
233 posO = 't'
234 posP = 'abhijkpqvwxyz'
235 posQ = '1'
236 posR = 'u'
237 posS = 'abhijkpqvwxyz'
238 posT = 'e'
239 posU = 'abhijkpqvwxyz'
240 posV = 'abhijkpqvwxyz'
241 posW = 'abhijkpqvwxyz'
242 posX = 'abhijkpqvwxyz'
243 posY = 'm'
244 posZ = 'c'
245 c = 0
246
247 # funcion para definir nuesto nuevo alfabeto quitando los caracteres encontrados
248 nuevoAlfabeto = 'abcdefghijklmnopqrstuvwxyz'
249 caracteresEncontrados = ['o','s','f','d','g','r','n','t','l','u','e','m','c']
250 for a in caracteresEncontrados:
251
         nuevoAlfabeto = nuevoAlfabeto.replace(a, "")
252 print (nuevoAlfabeto) # abhijkpqvwxyz
253
254 # probando en Gd
255 for p in dic:
256 if len(p) == 2:
257
           if (p[0] in posG and p[1] in posD):
258
                 print(p)
259
260 print(c)
261 # 1 resultado: if
```

```
Drive already mounted at /content/drive;
55900 palabras leidas
abhijkpqvwxyz
if
1
```

Probando con: yxwblgov

```
264 posA = 'abhjkpqvwxyz' # 0
265 posB = 'o'
266 posC = 's'
267 posD = 'f'
268 posE = 'd'
269 posF = 'abhjkpqvwxyz'
270 posG = 'i'
271 posH = 'abhjkpqvwxyz'
272 posI = 'g'
273 posJ = 'abhjkpqvwxyz'
274 posK = 'abhjkpqvwxyz'
275 posL = 'r'
276 posM = 'n'
277 posN = 'abhjkpqvwxyz'
278 pos0 = 't'
279 posP = 'abhjkpqvwxyz' # 0
280 posQ = '1'
281 posR = 'u'
282 posS = 'abhjkpqvwxyz' # 0
283 posT = 'e'
284 posU = 'abhjkpqvwxyz'
285 posV = 'abhjkpqvwxyz'
286 posW = 'abhjkpqvwxyz'
287 posX = 'abhjkpqvwxyz'
288 posY = 'm'
289 posZ = 'c'
290 c = 0
291
292 # funcion para definir nuesto nuevo alfabeto quitando los caracteres encontrados
293 nuevoAlfabeto = 'abcdefghijklmnopqrstuvwxyz'
294 caracteresEncontrados = ['o','s','f','d','i','g','r','n','t','l','u','e','m',
                            'c'1
296 for a in caracteresEncontrados:
297 | nuevoAlfabeto = nuevoAlfabeto.replace(a, "")
298 print (nuevoAlfabeto) # abhjkpqvwxyz
299
300 # probando en yxwblgov
301 for p in dic:
302 if len(p) == 8:
           if (p[0] in posY and p[1] in posX and p[2] in posW and p[3] in posB
303
               and p[4] in posL and p[5] in posG and p[6] in posO
304
305
                and p[7] in posV):
306
307
               print(p)
308 print(c)
309 # 1 resultado: majority
```

```
Drive already mounted at /content/drive;
55900 palabras leidas
abhjkpqvwxyz
majority
1
```

Probando con: bhkpqvwxz

```
312 posA = 'bhkpqvwxz' # 0
313 posB = 'o'
314 posC = 's'
315 posD = 'f'
316 posE = 'd'
317 posF = 'bhkpqvwxz'
318 pos6 = 'i'
319 posH = 'bhkpqvwxz'
320 posI = 'g'
321 posJ = 'bhkpqvwxz'
322 posK = 'bhkpqvwxz'
323 posL = 'r'
324 posM = 'n'
325 posN = 'bhkpqvwxz'
326 pos0 = 't'
327 posP = 'bhkpqvwxz' # 0
328 posQ = '1'
329 posR = 'u'
330 posS = 'bhkpqvwxz' # 0
331 posT = 'e'
332 posU = 'bhkpqvwxz'
333 posV = 'y'
334 posW = 'j'
335 posX = 'a'
336 posY = 'm'
337 posZ = 'c'
338 c = 0
339
340 # funcion para definir nuesto nuevo alfabeto quitando los caracteres encontrados
341 nuevoAlfabeto = 'abcdefghijklmnopqrstuvwxyz'
342 caracteresEncontrados = ['o','s','f','d','i','g','r','n','t','l','u','e','y',
344 for a in caracteresEncontrados:
345 | nuevoAlfabeto = nuevoAlfabeto.replace(a, "")
346 print (nuevoAlfabeto) # bhkpqvwxz
347
348 # probando en xqnxvc
349 for p in dic:
        if len(p) == 6:
            if (p[0] in posX and p[1] in posQ and p[2] in posN and p[3] in posX
351
352
                 and p[4] in posV and p[5] in posC):
353
354
               print(p)
355 print(c)
356 # 1 resultado: always
```

```
Drive already mounted at /content/drive;
55900 palabras leidas
bhkpqvwxz
always
1
```

Probando con: jtbjqt

```
359 posA = 'bhkpqvxz' # 0
360 posB = 'o'
361 posC = 's'
362 posD = 'f'
363 posE = 'd'
364 posF = 'bhkpqvxz'
365 posG = 'i'
366 posH = 'bhkpqvxz'
367 posI = 'g'
368 posJ = 'bhkpqvxz'
369 posK = 'bhkpqvxz'
370 posL = 'r'
371 posM = 'n'
372 posN = 'w'
373 pos0 = 't'
374 posP = 'bhkpqvxz' # 0
375 posQ = '1'
376 posR = 'u'
377 posS = 'bhkpqvxz' # 0
378 posT = 'e'
379 posU = 'bhkpqvxz'
380 posV = 'y'
381 posW = 'j'
382 posX = 'a'
383 posY = 'm'
384 posZ = 'c'
385 c = 0
386
387 # funcion para definir nuesto nuevo alfabeto quitando los caracteres encontrados
388 nuevoAlfabeto = 'abcdefghijklmnopqrstuvwxyz'
391 for a in caracteresEncontrados:
392 | nuevoAlfabeto = nuevoAlfabeto.replace(a, "")
393 print (nuevoAlfabeto) # bhkpqvxz
394
395 # probando en jtbjqt
396 for p in dic:
397 | if len(p) == 6:
         if (p[0] in posJ and p[1] in posT and p[2] in posB and p[3] in posJ
398
            and p[4] in posQ and p[5] in posT):
399
               c = c + 1
print(p)
400
401
402 print(c)
403 # 1 resultado: people
```

```
Drive already mounted at /content/drive; t
55900 palabras leidas
bhkpqvxz
people
1
```

Probando con: exiktco

```
453 posA = 'bhqvxz' # 0
454 posB = 'o'
455 posC = 's'
456 posD = 'f'
457 posE = 'd'
458 posF = 'bhqvxz' # tentativa VZ -> tftlvoigmu | E_ERYTGIN_
459 posG = 'i'
460 posH = 'bhqvxz'
461 posI = 'h'
462 #tftlvoigmu | E_ERYTGIN_ (no concuerda con que i sea g
463 #asi que se revisa y se cometió un error en la primera combinacion, ya
464 #se corrige en esta parte)
465 posJ = 'p'
466 posK = 'k'
467 posL = 'r'
468 posM = 'n'
469 posN = 'w'
470 pos0 = 't'
471 posP = 'bhqvxz' # 0
472 posQ = '1'
473 posR = 'u'
474 posS = 'bhqvxz' # 0
475 posT = 'e'
476 posU = 'bhqvxz'
477 posV = 'y'
478 posW = 'j'
479 posX = 'a'
480 posY = 'm'
481 posZ = 'c'
482 c = 0
483
484 # funcion para definir nuesto nuevo alfabeto quitando los caracteres encontrados
485 nuevoAlfabeto = 'abcdefghijklmnopqrstuvwxyz
486 caracteresEncontrados = ['o','s','f','d','i','g','p','k','r','n','w','t','l',
487 | | | | | | | 'u','e','y','j','a','m','c']
488 for a in caracteresEncontrados:
489 nuevoAlfabeto = nuevoAlfabeto.replace(a, "")
490 print (nuevoAlfabeto) # bhqvxz
491
492 # probando en htigme
493 for p in dic:
494 | if len(p) == 6:
495
        if (p[0] in posH and p[1] in posT and p[2] in posI and p[3] in posG
               and p[4] in posM and p[5] in posE):
496
497
                c = c + 1
498
               print(p)
499 print(c)
500 # 1 resultado: behind
```

```
Drive already mounted at /content/drive;
55900 palabras leidas
bhkqvxz
darkest
1
```

Probando con: htigmc

```
453 posA = 'bhqvxz' # 0
454 posB = 'o'
455 posC = 's'
456 posD = 'f'
457 posE = 'd'
458 posF = 'bhqvxz' # tentativa VZ -> tftlvoigmu | E_ERYTGIN_
459 posG = 'i'
460 posH = 'bhqvxz'
461 posI = 'h'
462 #tftlvoigmu | E_ERYTGIN_ (no concuerda con que i sea g
463 #asi que se revisa y se cometió un error en la primera combinacion, ya
464 #se corrige en esta parte)
465 posJ = 'p'
466 posK = 'k'
467 posL = 'r'
468 posM = 'n'
469 posN = 'w'
470 pos0 = 't'
471 posP = 'bhqvxz' # 0
472 posQ = '1'
473 posR = 'u'
474 posS = 'bhqvxz' # 0
475 posT = 'e'
476 posU = 'bhqvxz'
477 posV = 'y'
478 posW = 'j'
479 posX = 'a'
480 posY = 'm'
481 posZ = 'c'
482 c = 0
483
484 # funcion para definir nuesto nuevo alfabeto quitando los caracteres encontrados
485 nuevoAlfabeto = 'abcdefghijklmnopqrstuvwxyz
486 caracteresEncontrados = ['o','s','f','d','i','g','p','k','r','n','w','t','l',
487 | | | | | | | | | | 'u','e','y','j','a','m','c']
488 for a in caracteresEncontrados:
489 | nuevoAlfabeto = nuevoAlfabeto.replace(a, "")
490 print (nuevoAlfabeto) # bhqvxz
491
492 # probando en htigme
493 for p in dic:
        if len(p) == 6:
            if (p[0] in posH and p[1] in posT and p[2] in posI and p[3] in posG
495
                and p[4] in posM and p[5] in posE):
496
497
498
                print(p)
499 print(c)
500 # 1 resultado: behind
```

```
Drive already mounted at /content/drive;
55900 palabras leidas
bhqvxz
behind
1
```

Probando con: ybfgmu

```
503 posA = 'gqvxz' # 0
504 posB = 'o'
505 posC = 's'
506 posD = 'f'
507 posE = 'd'
508 posF = 'gqvxz'
509 posG = 'i'
510 posH = 'b'
511 posI = 'h'
512 posJ = 'p'
513 posK = 'k'
514 posL = 'r'
515 posM = 'n'
516 posN = 'w'
517 pos0 = 't'
518 posP = 'gqvxz' # 0
519 posQ = '1'
520 posR = 'u'
521 posS = 'gqvxz' # 0
522 posT = 'e'
523 posV = 'gqvxz'
524 posV = 'y'
525 posW = 'j'
526 posX = 'a'
527 posY = 'm'
528 posZ = 'c'
529 c = 0
530
531 # funcion para definir nuesto nuevo alfabeto quitando los caracteres encontrados
532 nuevoAlfabeto = 'abcdefghijklmnopqrstuvwxyz'
533 caracteresEncontrados = ['o','s','f','d','i','b','h','p','k','r','n','w','t',
534 | | | | | | | | 'l','u','e','y','j','a','m','c']
535 for a in caracteresEncontrados:
536 nuevoAlfabeto = nuevoAlfabeto.replace(a, "")
537 print (nuevoAlfabeto) # gqvxz
538
539 # probando en ybfgmu
540 for p in dic:
541 | if len(p) == 6:
            if (p[0] in posY and p[1] in posB and p[2] in posF and p[3] in posG
542
543
            and p[4] in posM and p[5] in posU):
544
545
                print(p)
546 print(c)
547 # 1 resultado: moving
```

```
Drive already mounted at /content/drive;
55900 palabras leidas
gqvxz
moving
1
```

Ya tendríamos todo el abecedario

```
550 posA = 'X' # 0
551 posB = 'o'
552 posC = 's'
553 posD = 'f'
554 posE = 'd'
555 posF = 'v'
556 posG = 'i'
557 posH = 'b'
558 posI = 'h'
559 posJ = 'p'
560 posK = 'k'
561 posL = 'r'
562 posM = 'n'
563 posN = 'w'
564 pos0 = 't'
565 posP = 'X' # 0
566 posQ = '1'
567 posR = 'u'
568 posS = 'X' # 0
569 posT = 'e'
570 posU = 'g'
571 posV = 'y'
572 posW = 'j'
573 posX = 'a'
574 posY = 'm'
575 posZ = 'c'
```

alfabeto = abcdefghijklmnopgrstuvwxyz

Llave = XosfdvibhpkrnwtXluXegyjamc

Finalmente usamos la función de descifraSustituye() mandando como parámetros la llave y la cadena (texto cifrado), y finalmente la función nos va a retornar el texto descifrado.

```
580 alfabetoFinal = "XosfdvibhpkrnwtXluXegyjamc"
581 print (descifraSustituye(cifrado,alfabetoFinal))
```

donde cifrado contiene el texto:

Oitlt xlt onb ovjtc bd jtbjqt nib ngqq otqq vbr oixo vbr zxmmbo yxkt x egddtltmzt gm oigc nblqe: oibct nib xlt xdlxge ob olv xme oibct nib xlt xdlxge vbr ngqq crzztte Crzztcc gc qgkgmu vbrlctqd, qgkgmu nixo vbr eb, xme qgkgmu ibn vbr eb go Nitmtftl vbr dgme vbrlctqd bm oit cget bd oit yxwblgov, go gc ogyt ob jxrct xme ltdqtzo Kttj vbrl dxzt xqnxvc obnxle oit crmcigmt xme cixebnc ngqq dxqq htigme vbr Gd vbr ixft tftlvoigmu rmetl zbmolbq, vbr xlt mbo ybfgmu dxco tmbrui Go gc erlgmu brl exlktco ybytmoc oixo nt yrco dbzrc ob ctt oit qguio

Que descifrado sería:

there are two types of people who will tell you that you cannot make a difference in this world: those who are afraid to try and those who are afraid you will succeed success is liking yourself, liking what you do, and liking how you do it whenever you find yourself on the side of the majority, it is time to pause and reflect keep your face always toward the sunshine and shadows will fall behind you if you have everything under control, you are not moving fast enough it is during our darkest moments that we must focus to see the light

Traducido al español:

hay dos tipos de personas que te dirán que no puedes marcar la diferencia en este mundo: los que tienen miedo de intentarlo y los que tienen miedo de que tengas éxito el éxito es gustarte a ti mismo, gustarte lo que haces y gustarte cómo lo haces siempre que te encuentres en el lado de la mayoría, es el momento de hacer una pausa y reflexionar mantén tu cara siempre hacia el sol y las sombras caerán detrás de ti si todo bajo control, te estás moviendo no momentos más suficientemente rápido es durante nuestros oscuros cuando debemos centrarnos para ver la luz

TEXTO 2:

Texto cifrado:

Jz bzz qwjjd ped nevvd le vkzhd eo mod hdlvd kelwkhd odvmkdjw d neknd hwove naejzpwvke qe qelvdobd. Vmvvd jd bzod w qwjepevdvd odvmkdjpwovw qd gdkwve kznnezlw z kegeqe gwoqee, umeoqe gwk jd pdffezk gdkvw qwfje doepdje ozo lzoz ownwlldkew fdccew, ow lgwnedje kwneolezoe. Lzjz rwjeoe dcevdoz j'oend gdkvw naemld, naw ad qe rdjvz jd lvwlld vkelvwbd qwe jzkz znnae kdllwfodve. Lzoz dggwod dkkehdvz eo Evdjed wq w mo jmzfz qdhhwkz eondovwhzjw. Ewke az helevdvz ej nwovkz qe Kzpd w qwhz qekw naw w qdhhwkz mod nevvd nzo pzjve pzompwove dovenae, eordvve lzoz keldjwove djj wgznd Kzpdod. Az helvz ej Nzjzllwz w qwhz dppwvvwkw naw gwoldhz rzllw gem gennzjz, eohwnw w fkdoqw wq w qdhhwkz mo cwj pzompwovz, gwnndvz naw ozo lzoz kemlnevz dq wovkdkw.

(idioma detectado: Italiano)

Código:

```
def cargaPalabras():
         archivo = open('italiano diccionario.txt', 'r')
         renglon = archivo.readline()
         palabras = renglon.split()
         print (len(palabras), 'palabras leidas')
         return palabras
    def cargaCifrado():
         archivo = open('cifrado.txt', 'r')
         renglon = archivo.readline()
         return renglon
    def descifraSustituye(cadena, alfabetoLlave):
         alfabeto = 'abcdefghijklmnopqrstuvwxyz'
         nuevaCadena = ""
         for letra in cadena:
             if letra in alfabeto:
                 posicion = alfabetoLlave.find(letra)
                 nuevaCadena = nuevaCadena + alfabeto[posicion]
                 nuevaCadena = nuevaCadena + letra
         return nuevaCadena
26 dic = cargaPalabras()
27   cifrado = cargaCifrado()
28 histo = {}
29 alfabeto = 'abcdefghijklmnopqrstuvwxyz'
    for e in alfabeto:
         histo[e] = 0
     for letra in cifrado:
         if letra in alfabeto:
             histo[letra] += 1
     print(histo)
```

La salida del histograma del Texto cifrado 2, es el siguiente:

{'a': 10, 'b': 4, 'c': 4, 'd': 70, 'e': 69, 'f': 7, 'g': 14, 'h': 18, 'i': 0, 'j': 29, 'k': 33, 'l': 28, 'm': 14, 'n': 29, 'o': 48, 'p': 15, 'q': 22, 'r': 4, 's': 0, 't': 0, 'u': 1, 'v': 44, 'w': 68, 'x': 0, 'y': 0, 'z': 59}

En el texto cifrado 2, gracias al histograma de frecuencias, omitimos 5 posibles letras: i, s, t, x, y; además, como en el idioma italiano no existen las letras: J, K, W, X, Y, podemos omitirlas de las letras que buscamos, quedándonos de la siguiente manera:

posA="abcdefghilmnopqrstuvz" posB="abcdefghilmnopqrstuvz" posC="abcdefghilmnopqrstuvz" posD="abcdefghilmnopgrstuvz" posE="abcdefghilmnopgrstuvz" posF="abcdefghilmnopgrstuvz" posG="abcdefghilmnopgrstuvz" posH="abcdefghilmnopqrstuvz" posJ="abcdefghilmnopgrstuvz" posK="abcdefghilmnopgrstuvz" posL="abcdefghilmnopqrstuvz" posM="abcdefghilmnopgrstuvz" posN="abcdefghilmnopgrstuvz" posO="abcdefghilmnopgrstuvz" posP="abcdefghilmnopqrstuvz" posQ="abcdefghilmnopqrstuvz" posR="abcdefghilmnopqrstuvz" posU="abcdefghilmnopqrstuvz" posV="abcdefghilmnopqrstuvz" posW="abcdefghilmnopgrstuvz" posZ="abcdefghilmnopqrstuvz"



Probando con: dppwvvwkw

```
posA="abcdefghilmnopqrstuvz"
      posB="abcdefghilmnopqrstuvz"
 posC="abcdefghilmnopqrstuvz"
posD="abcdefghilmnopqrstuvz"
 posE="abcdefghilmnopqrstuvz"
posF="abcdefghilmnopqrstuvz"
posG="abcdefghilmnopqrstuvz"
 post="abcdefghilmnopqrstuvz"
post="abcdefghilmnopqrstuvz"
post="abcdefghilmnopqrstuvz"
posK="abcdefghilmnopqrstuvz"
      posM="abcdefghilmnopqrstuvz"
posN="abcdefghilmnopqrstuvz"
      posP="abcdefghilmnopqrstuvz"
posQ="abcdefghilmnopqrstuvz"
 56 posR="abcdefghilmnopqrstuvz"
      posU="abcdefghilmnopqrstuvz"
posV="abcdefghilmnopqrstuvz"
      posW="abcdefghilmnopqrstuvz"
       posZ="abcdefghilmnopqrstuvz"
              if len(p)==9:
                 if p[1]==p[2] and p[3]==p[6] and p[3]==p[-1] and p[4]==p[5]:
                        print(p)
       print("Num palabras: ",c)
 PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
affannata
allessere
ammettere
annettere
appannata
attaccata
avvizziti
eccellere
occorrono
Num palabras: 10
PS C:\Users\JosueManzano\Desktop\DescifradoItaliano>
```

Palabras Validas:

- allessere
- ammettere
- annettere
- avvizziti

- posD: a
- posP: lmnv
- posW: ei
- posV: stz
- posK: rt

Probando con: ownwlldkew

```
#PROBANDO CON: ownwlldkew
      posA="abcdefghilmnopqrstuvz"
      posB="abcdefghilmnopqrstuvz"
      posC="abcdefghilmnopqrstuvz"
      posD="a"
      posE="abcdefghilmnopqrstuvz"
      posF="abcdefghilmnopqrstuvz"
      posG="abcdefghilmnopqrstuvz"
      posH="abcdefghilmnopqrstuvz"
      posJ="abcdefghilmnopqrstuvz"
      posK="rt"
      posL="abcdefghilmnopqrstuvz"
      posM="abcdefghilmnopqrstuvz"
      posN="abcdefghilmnopqrstuvz"
      pos0="abcdefghilmnopqrstuvz"
      posP="lmnv"
      posQ="abcdefghilmnopqrstuvz"
      posR="abcdefghilmnopqrstuvz"
      posU="abcdefghilmnopqrstuvz"
      posV="stz"
      posW="ei"
      posX="abcdefghilmnopqrstuvz"
      C=0
      for p in dic:
          if len(p)==10:
 98
              if p[1] in posW and p[1]==p[3] and p[1]==p[-1] and p[-4]=='a' and p[4]==p[5]:
                  c+=1
                  print(p)
      print("Num palabras: ",c)
          OUTPUT DEBUG CONSOLE
                                 TERMINAL
necessarie
PS C:\Users\JosueManzano\Desktop\DescifradoItaliano>
```

Palabras Validas:

necessarie

- posO: n
- posW: e
- posN: c
- posL: s
- posD: a
- posK: r
- posE: i

Probando con: Nzjzllwz

```
posA="abcdefghilmnopqrstuvz"
141 posB="abcdefghilmnopqrstuvz"
142 posC="abcdefghilmnopqrstuvz"
     posD="a"
     posE="i"
      posF="abcdefghilmnopqrstuvz"
     posG="abcdefghilmnopqrstuvz"
147 posH="abcdefghilmnopqrstuvz"
     posJ="abcdefghilmnopqrstuvz"
     posK="r"
      posL="s"
     posM="abcdefghilmnopqrstuvz"
     posN="c"
153 pos0="n"
154 posP="lmnv"
     posQ="abcdefghilmnopqrstuvz"
      posR="abcdefghilmnopqrstuvz"
      posU="abcdefghilmnopqrstuvz"
     posV="stz"
      posW="e"
      posZ="abcdefghilmnopqrstuvz"
      C=0
      for p in dic:
          if len(p)==8:
              if p[0]=='c' and p[1]==p[3] and p[1]==p[-1] and p[-3]=='s' and p[4]==p[5]:
                  C+=1
                  print(p)
      print("Num palabras: ",c)
                  DEBUG CONSOLE
                                TERMINAL
colosseo
Num palabras: 1
PS C:\Users\JosueManzano\Desktop\DescifradoItaliano> [
```

Palabras validas:

colosseo

- posZ: o
- posJ: I

Probando con: gennzjz

```
posA="bdfghmpqtuvz"
141 posB="bdfghmpqtuvz"
142 posC="bdfghmpqtuvz"
143 posD="a"
144 posE="i"
145 posF="bdfghmpqtuvz"
146 posG="bdfghmpqtuvz"
147 posH="bdfghmpqtuvz"
148 posJ="1"
149 posK="r"
150 posL="s"
     posM="bdfghmpqtuvz"
     posN="c"
153 pos0="n"
154 posP="mv"
155 posQ="bdfghmpqtuvz"
156    posR="bdfghmpqtuvz"
157 posU="bdfghmpqtuvz"
158 posV="tz"
159 posW="e"
160 posZ="o"
     C=0
      for p in dic:
      if len(p)==7:
             if p[-1]==p[-3] and p[-1]=='o' and p[2]==p[3] and p[2]=='c' and p[-2]=='l' and p[1]=='i':
                  c+=1
                 print(p)
168 print("Num palabras: ",c)
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
niccolo
piccolo
Num palabras: 2
PS C:\Users\JosueManzano\Desktop\DescifradoItaliano> [
```

Palabras validas:

- niccolo
- piccolo

Reducción de Posibles combinaciones:

posG: p

```
posA="bdfghmqtuvz"
     posB="bdfghmqtuvz"
      posC="bdfghmqtuvz"
     posD="a"
     posE="i"
     posF="bdfghmqtuvz"
      posG="p"
      posH="bdfghmqtuvz"
    posJ="1"
     posK="r"
     posL="s"
      posM="bdfghmqtuvz"
     posN="c"
     pos0="n"
      posP="mv"
      posQ="bdfghmqtuvz"
    posR="bdfghmqtuvz"
190 posU="bdfghmqtuvz"
191 posV="tz"
      posW="e"
      posZ="o"
      for p in dic:
          if len(p)==12:
              if p[0]=='n' and p[4]=='r' and p[1]=='a' and p[-4]==p[-1] and p[-1]=='e':
                  print(p)
      print("Num palabras: ",c)
PROBLEMS OUTPUT DEBUG CONSOLE
                                TERMINAL
naturalmente
Num palabras: 1
PS C:\Users\JosueManzano\Desktop\DescifradoItaliano> [
```

Palabras validas:

naturalmente

Reducción de Posibles combinaciones:

posV: tposM: uposP: m

Probando con: qelvdobd

```
posA="bdfghmqt"
    posB="bdfghmqt"
210 posC="bdfghmqt"
211 posD="a"
212 posE="i"
213 posF="bdfghmqt"
214 posG="p"
215 posH="bdfghmqt"
216 posJ="1"
217 posK="r"
218 posL="s"
     posM="u"
     posN="c"
     pos0="n"
222 posP="m"
223 posQ="bdfghmqt"
224 posR="bdfghmqt"
225 posU="bdfghmqt"
226 posV="t"
227 posW="e"
228 posZ="o"
     for p in dic:
         if len(p)==8:
             if p[1]=='i' and p[3]=='t' and p[2]=='s' and p[-4]==p[-1] and p[-3]=='n' and p[-1]=='a':
                 c+=1
                print(p)
236 print("Num palabras: ",c)
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
distanza
Num palabras: 1
PS C:\Users\JosueManzano\Desktop\DescifradoItaliano> []
```

Palabras validas:

distanza

Reducción de Posibles combinaciones:

posQ: dposB: z

Probando con: dovenae

```
posA="bfghqv"
    posB="z"
243 posC="bfghqv"
244 posD="a"
245 posE="i"
246 posF="bfghqv"
247 posG="p"
248 posH="bfghqv"
249 posJ="1"
     posK="r"
251 posL="s"
252 posM="u"
253 posN="c"
254 pos0="n"
255 posP="m"
259 posV="t"
260 posW="e"
261 posZ="o"
263 c=0
     if len(p)==7:
            if p[0]=='a' and p[1]=='n' and p[2]=='t' and p[-4]==p[-1] and p[-1]=='i' and p[-2] in posA:
                C+=1
                print(p)
269 print("Num palabras: ",c)
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
antichi
Num palabras: 1
PS C:\Users\JosueManzano\Desktop\DescifradoItaliano>
```

Palabras validas:

antichi

Reducción de Posibles combinaciones:

posA: h

Probando con: umeoqe

```
#PROBANDO CON: umeoge
     posA="h"
    posB="z"
    posC="bfgqv"
     posD="a"
     posE="i"
    posF="bfgqv"
     posG="p"
     posH="bfgqv"
     posJ="1"
     posK="r"
     posL="s"
    posM="u"
    posN="c"
288 pos0="n"
     posP="m"
    posQ="d"
    posR="bfgqv"
    posU="bfgqv"
     posV="t"
     posW="e"
     posZ="o"
     C=0
     for p in dic:
          if len(p)==6:
             if p[0] in posU and p[1]=='u' and p[2]=='i' and p[-4]==p[-1] and p[-1]=='i':
                 c+=1
                 print(p)
     print("Num palabras: ",c)
303
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
quinci
quindi
quinti
Num palabras: 3
PS C:\Users\JosueManzano\Desktop\DescifradoItaliano>
```

Palabras validas:

- quinci
- quindi
- quinti

Reducción de Posibles combinaciones:

posU: q

Probando con: dkkehdvz

```
#PROBANDO CON: dkkehdvz
     posA="h"
     posB="z"
311 posC="bfgv"
312 posD="a"
313 posE="i"
     posF="bfgv"
315 posG="p"
316 posH="bfgv"
317 posJ="1"
     posK="r"
    posL="s"
320 posM="u"
321 posN="c"
     pos0="n"
323 posP="m"
324 posQ="d"
325 posR="bfgv"
     posU="q"
     posV="t"
328 posW="e"
329 posZ="o"
332 for p in dic:
         if len(p)==8:
             if p[0]=='a' and p[1]=='r' and p[3]=='i' and p[1]==p[2] and p[-1]=='o':
                 c+=1
                 print(p)
337 print("Num palabras: ",c)
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
arrivato
Num palabras: 1
PS C:\Users\JosueManzano\Desktop\DescifradoItaliano> []
```

Palabras validas:

arrivato

Reducción de Posibles combinaciones:

posH: v

Probando con: qwfje

```
340
      #PROBANDO CON: qwfje
      posA="h"
      posB="z"
      posC="bfg"
      posD="a"
      posE="i"
      posF="bfg"
      posG="p"
      posH="v"
      posJ="1"
      posK="r"
      posL="s"
      posM="u"
      posN="c"
      pos0="n"
      posP="m"
      posQ="d"
      posR="bfg"
      posU="q"
      posV="t"
      posW="e"
      posZ="o"
      #PROBANDO CON: qwfje
      C=0
      for p in dic:
         if len(p)==5:
              if p[0]=='d' and p[1]=='e' and p[-2]=='l' and p[-1]=='i':
                  c+=1
                  print(p)
370 print("Num palabras: ",c)
         OUTPUT DEBUG CONSOLE
                                 TERMINAL
degli
delli
Num palabras: 2
PS C:\Users\JosueManzano\Desktop\DescifradoItaliano>
```

Palabras validas:

- degli
- delli

Reducción de Posibles combinaciones:

posF: g

Probando con: dcevdoz

```
#PROBANDO CON: dcevdoz
375 posA="h"
376 posB="z"
    posC="bf"
378 posD="a"
     posE="i"
     posF="g"
    posG="p"
382 posH="v"
383 posJ="1"
     posK="r"
    posL="s"
386 posM="u"
     posN="c"
      pos0="n"
389 posP="m"
390 posQ="d"
     posR="bf"
     posU="q"
393 posV="t"
     posW="e"
      posZ="o"
     #PROBANDO CON: dcevdoz
     C=0
     for p in dic:
          if len(p)==7:
             if p[0]=='a' and p[2]=='i' and p[0]==p[-3] and p[-2]=='n' and p[-1]=='o':
                 c+=1
                 print(p)
      print("Num palabras: ",c)
PROBLEMS OUTPUT DEBUG CONSOLE
                               TERMINAL
abitano
Num palabras: 1
PS C:\Users\JosueManzano\Desktop\DescifradoItaliano> []
```

Palabras validas:

abitano

- posC: b
- posR: f

Las posibles letras nos quedan de la siguiente forma:

```
posA="h"
posB="z"
posC="b"
posD="a"
posE="i"
posF="g"
posG="p"
posH="v"
posJ="l"
posK="r"
posL="s"
posM="u"
posN="c"
posO="n"
posP="m"
posQ="d"
posR="f"
posU="q"
posV="t"
posW="e"
posZ="o"
```

```
posA="h" posB="z" posC="b" posD="a" posE="i" posF="g" posG="p" posH="v" posJ="l"

posK="r" posL="s" posM="u" posN="c" posO="n" posP="m" posQ="d" posR="f" posU="q"

posV="t" posW="e" posZ="o"
```

Ahora vamos armando nuestra llave. Para armar la llave escribimos el alfabeto:

abcdefghijklmnopqrstuvwxyz

Y para cada letra buscamos su original, por ejemplo, en el caso de la "a":

```
posA="h" posB="z" posC="b" posD="a" posE="i" posF="g" posG="p" posH="v" posJ="l"

posK="r" posL="s" posM="u" posN="c" posO="n" posP="m" posQ="d" posR="f" posU="q"

posV="t" posW="e" posZ="o"
```

Vemos que en el texto cifrado apareció una "D" en sustitución de la "a", por lo que la escribimos

debajo de la "a":

abcdefghijklmnopqrstuvwxyz

d

Ahora buscamos a "b" y reemplazamos, y así sucesivamente, excepto con las letras que no aparecen, donde podemos poner una X:

```
        posA="h"
        posB="z"
        posC="b"
        posD="a"
        posE="i"
        posF="g"
        posG="p"
        posH="v"

        posJ="I"
        posK="r"
        posL="s"
        posM="u"
        posN="c"
        posO="n"
        posP="m"
        posQ="d"
        posR="f"

        posV="t"
        posW="e"
        posZ="o"
```

Alfabeto:

abcdefghijklmnopgrstuvwxyz

Llave:

dcnqwrfae XXjpozguklvmh XXXb

Finalmente usamos la función de **descifraSustituye()** mandando como parámetros la llave y la cadena (texto cifrado), y finalmente la función nos va a retornar el texto descifrado.

```
llave='dcnqwrfaeXXjpozguklvmhXXXb'

cadena="Jz bzz qwjjd ped nevvd le vkzhd eo mod hdlvd kelwkhd odvmkdjw d neknd hwove naejzpwvke qe qelvdobd. "\

""mvvd jd bzod w qwjepevdvd odvmkdjpwovw qd gdkwve kznnezlw z kegeqe gwoqee, umeoqe gwk jd pdffezk "\

"gdkvw qwfje doepdje ozo lzoz ownwlldkew fdccew, ow lgwnedje kwneolezoe. Lzjz rwjeoe dcevdoz j'oend "\

"gdkvw naemld, naw ad qe rdjvz jd lvwlld vkelvwbd qwe jzkz znnae kdllwfodve. Lzoz dggwod dkkehdvz eo "\

"Evdjed wq w mo jmzfz qdhhwkz eondovwhzjw. Ewke az helevdvz ej nwovkz qe Kzpd w qwhz qekw naw w qdhhwkz "\

"mod nevvd nzo pzjve pzompwove dovenae, eordvve lzoz keldjwove djj wgznd Kzpdod. Az helvz ej Nzjzllwz w qwhz "\

"dpwvvwku naw gwoldhz rzllw gem gennzjz, eohwnw w fkdoqw wq w qdhhwkz mo cwj pzompwovz, gwnndvz naw ozo lzoz kemlnevz dq wovkdkw."

b=descifraSustituye(cadena, llave)

print("\nTexto Descifrado por Sustitucion: ")

print(b)
```

```
Texto Descifrado por Sustitucion:

Jo zoo della mia citta si trova in una vasta riserva naturale a circa venti chilometri di distanza. Vutta la zona e delimitata naturalmente da pareti ro cciose o ripidi pendii, quindi per la maggior parte degli animali non sono necessarie gabbie, ne speciali recinsioni. Lolo felini abitano l'nica parte c hiusa, che ha di falto la stessa tristeza dei loro occhi rassegnati. Lono appena arrivato in Etalia ed e un luogo davvero incantevole. Eeri ho visitato il centro di Koma e devo dire che e davvero una citta con molti monumenti antichi, infatti sono risalenti all epoca Komana. Ao visto il Nolosseo e devo ammettere che pensavo fosse piu piccolo, invece e grande ed e davvero un bel monumento, peccato che non sono riuscito ad entrare.

PS C:\Users\JosueManzano\Desktop\DescifradoItaliano> \[ \bigcirc \text{ O Prettier } \Displace \text{ In 33, Col 26 Spaces: 4 UTF-8 CRLF (\bigcirc} \text{ Python } 3.11.4 64-bit \text{ \text{ O G Live } \text{ O Prettier } \Displace \text{ In 33, Col 26 Spaces: 4 UTF-8 CRLF (\bigcirc} \text{ Python } 3.11.4 64-bit \text{ \text{ O G Live } \text{ O Prettier } \Displace \Displace \text{ O Prettier } \Displace \Displace
```

Texto Descifrado del italiano:

lo zoo della mia citta si trova in una vasta riserva naturale a circa venti chilometri di distanza. tutta la zona e delimitata naturalmente da pareti rocciose o ripidi pendii, quindi per la maggior parte degli animali non sono necessarie gabbie, ne speciali recinsioni. solo felini abitano l'nica parte chiusa, che ha di falto la stessa tristeza dei loro occhi rassegnati. sono appena arrivato in italia ed e un luogo davvero incantevole. ieri ho visitato il centro di roma e devo dire che e davvero una citta con molti monumenti antichi, infatti sono risalenti all'epoca romana. ho visto il colosseo e devo ammettere che pensavo fosse piu piccolo, invece e grande ed e davvero un bel monumento, peccato che non sono riuscito ad entrare.

Texto descifrado traducido al español:

El zoológico de mi ciudad está situado en una gran reserva natural a unos veinte kilómetros de distancia. Toda la zona está delimitada naturalmente por paredes rocosas o pendientes pronunciadas, por lo que para la mayoría de los animales no son necesarias jaulas ni recintos especiales. sólo felinos habitan la única parte cerrada, que tiene la misma tristeza que sus ojos resignados. Acabo de llegar a Italia y es un lugar verdaderamente encantador. ayer visité el centro de Roma y debo decir que verdaderamente es una ciudad con muchos monumentos antiguos, de hecho datan de la época romana. Vi el Coliseo y debo admitir que pensé que era más pequeño, pero en cambio es grande y es realmente un monumento hermoso, lástima que no pude entrar.