

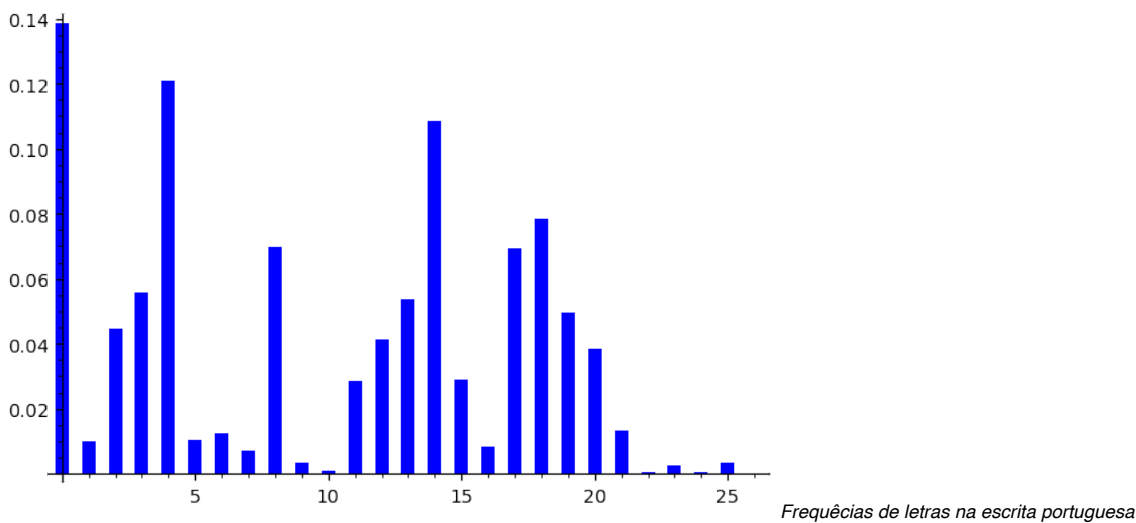
Week 1 – 23/09/2022

Exercício 1

Primeiro começamos por compara as frequências de cada letra na cifra com a frequência de cada letra em textos deste tipo (portugueses). Depois ordenamos as letras por ordem decrescente de frequências.

```
from data import *

display(bar_chart([Stats[c] for c in string.ascii_lowercase]))
```



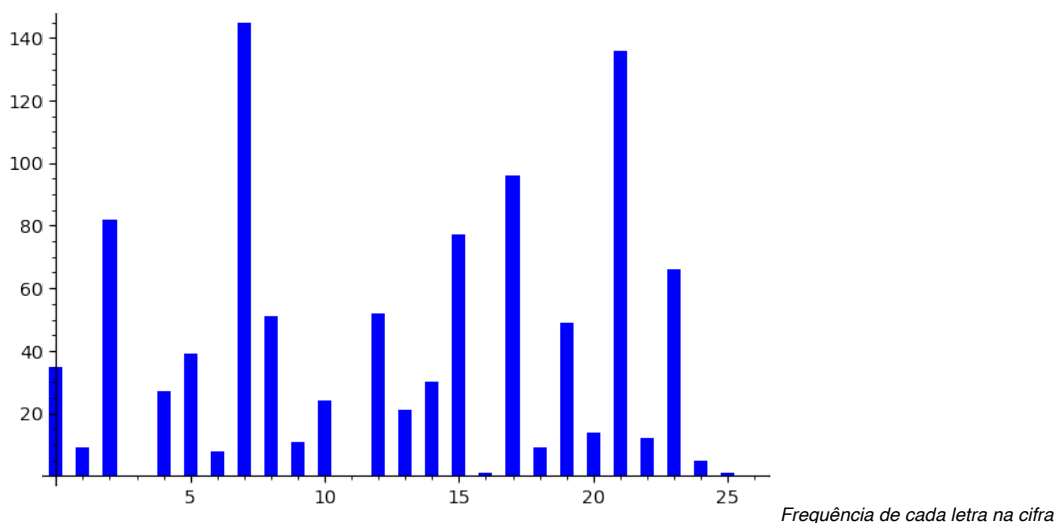
A mensagem foi convertida em código numérico: 'a'→1, 'b'→2,...

```
d=dict()

for i in range(1,27):
    d[i] = 0

for i in msg1:
    d[i] += 1

display(bar_chart([d[i] for i in range(1,27)]))
print({k: v for k, v in sorted(Stats.items(), key=lambda item: item[1])})
print({k: v for k, v in sorted(d.items(), key=lambda item: item[1])})
```



{'w': 0.000463854585819342, 'y': 0.000539614263910087, 'k': 0.000818787290134591, 'x': 0.00240197030664632, 'z': 0.0032743166366033, 'j': 0.00352573886499237, 'h': 0.00713098376578327, 'q': 0.00836325794366588, 'b': 0.00992854169557375, 'f': 0.010520743721382, 'g': 0.0126298043568753, 'v': 0.0133593728319689, 'l': 0.0286513112251977, 'p': 0.0291236298043569, 'u': 0.0385138060219231, 'm': 0.0414230609130012, 'c': 0.0447716109338143, 't': 0.0495047870126266, 'n': 0.0538477868738726, 'd': 0.0558000555015957, 'r': 0.069451089218815, 'i': 0.0698455668100458, 's': 0.0782698765089496, 'o': 0.108550992091023, 'e': 0.120706257804912, 'a': 0.138583183016512}

{4: 0, 12: 0, 17: 1, 26: 1, 25: 5, 7: 8, 2: 9, 19: 9, 10: 11, 23: 12, 21: 14, 14: 21, 11: 24, 5: 27, 15: 30, 1: 35, 6: 39, 20: 49, 9: 51, 13: 52, 24: 66, 16: 77, 3: 82, 18: 96, 22: 136, 8: 145}

Depois associamos as frequências e tentamos decifrar a mensagem fazendo modificações na associação de letras até descobrirmos a chave.

Chave:

a=c,b=q,c=s,d=w,e=l,f=t,g=z,h=e,i=d,j=h,k=p,l=y,m=n,n=g,o=u,p=r,k=k,r=o,s=b,t=m,u=v,v=a,w=f,x=i,y=j,z=x

Mensagem decifrada:

```
for c in msg1:
    letras=['c','q','s','w','l','t','z','e','d','h','p','y','n','g','u','r','k','o','b','m','v','a','f','i','j','x']
    print(letras[c-1],end="")
```

oposicaoemminhapropriacasaondealgumqueinsisteemseralergicominhamiseravelvidameperguntaregularmenteenaohouvenadadebomquelhetenhaacontecidofredausterlitzvirginia

oposicao em minha propria casa onde algum que insiste em ser alergico minha miseravel vida me pergunta regularmente e nao houve nada de bom que lhe tenha acontecido fred austerlitz e virginia katherine mcmath sao nomes nada significam para a maioria das pessoas mas se lhes pusermos umas claquetes nos sapatos da se uma operacao de magia e surgem fred astaire e ginger rogers o estilo e a elegancia por excelencia no reino da danca a esse reino que a cinema tecanos transporta ao recordar de a de fevereiro nove dos dez filmes que fizeram juntos hoje presidente da república mario soares foi um dos adversarios politicos de pinto balsemao era nessa altura secretario geral do partido socialista e como tal lider da oposicao parlamentar ao governo da alianca democratica que balsemao chefiou de de janeiro de a de junho de renunciou ao cargo a de dez em brode mas manteve se em funcoes mais cinco meses ate a posse do novo governo apos a morte subita de sa carneiro a de dezembro de dez anos passados mario soares escreve sobre o seu antigo adversario mas tambem aliado e amigo em momentos que ele proprio faz questao de assinalar dos dez filmes que fred astaire e ginger rogers interpretaram dancaram juntos va

Exercício 2

Determinamos o tamanho da chave, calculando os divisores comuns dos períodos com que um sequência de letras se repetia.

```
print('a chave divide:')
for p in range (997):
    for q in range (996-p):
        if [msg2[p],msg2[p+1],msg2[p+2],msg2[p+3]]==[msg2[p+q+1],msg2[p+q+2],msg2[p+q+3],msg2[p+q+4]]:
            print(q+1,end=',')
```

a chave divide: 635,635,635,390,390,425,415,305,90,90,90,215,215,215,90,310,190,275,190,275,190,275,190,275,275,155,155,155,85,85,85,85,15,

Os divisores comuns são 5 e 1, logo a palavra deve ter comprimento 5.

Descobrimos a chave tentando combinações de 5 letras até a mensagem fazer sentido.

Chave:

pefvi

Mensagem decifrada:

```
aux=[ord('p')-97,ord('e')-97,ord('f')-97,ord('v')-97,ord('i')-97]*200
tab = [[0]*26 for i in range(26)]
for p in range (26):
    tab[p]=list(range(p,26))+list(range(p))
msg2alt=copy(msg2)
for t in range (1000):
    msg2alt[t]=msg2[t]-1

msg2fin=copy(msg2alt)
for q in range(1000):
    for w in range(26):
        if tab[w][aux[q]]==msg2alt[q]:
            msg2fin[q]=chr(w+97)
    print(msg2fin[q],end='')
```

eportuguesestreiaseassimcomoprofissionalnoseupaisenoteatronacionaldedmariaiparaasublimemariaseramaisumarepresentacaodezazouqueestahalargosmesesemcenaemparisp

Exercício 3

```
print('divisor de:')
for p in range (997):
    for q in range (996-p):
        if [msg3[p],msg3[p+1],msg3[p+2],msg3[p+3]]==[msg3[p+q+1],msg3[p+q+2],msg3[p+q+3],msg3[p+q+4]]:
            print(q+1,end=',')
```

Chave de comprimento 12:

Mensagem decifrada:

```
aux=[ord('f')-97,ord('w')-97,ord('q')-97,ord('i')-97,ord('r')-97,ord('t')-97,ord('u')-97,ord('n')-97,ord('c')-97,ord('p')-97,ord(
tab = [[0]*26] for i in range(26)]
for p in range (26):
    tab[p]=list(range(p,26))+list(range(p))
msg3alt=copy(msg3)
for t in range (1000):
    msg3alt[t]=msg3[t]-1

msg3fin=copy(msg3alt)
for q in range(1000):
    for w in range(26):
        if tab[w][aux[q]]==msg3alt[q]:
            msg3fin[q]=chr(w+97)
    print(msg3fin[q],end='')
```

essa parlamentar de negocios estrangeiros destinada a analisar a guerra no golfo joao de deus pinheiro tomou ontem a iniciativa de desdramatizar a recente diligencia diplomatica de mario soares junto de yasser arafat frisando que a atitude do presidente da republica nao provocou nenhum remoo que nos parceiros comunitarios sem que alguem lhe tenha suscitado o assunto o ministro informou que no ultimo conselho de negocios estrangeiros da cee ninguem levantou problemas relativamente a iniciativa do prntem de manha crespo chamou e ao seu gabinete e explicou lhe so ter tido conhecimento na terca feira a tarde dos dois pedidos de deslocacao o que amaral estranhou ja que te lo a formalizado ha um mes ao gabinete do presidente tais pedidos so terao no entanto chegado na segunda feira a noite o que fundamentou a justificacao para o atrazo dirigentes da maioria nao poupam no entanto victor crespo a acusacoes de ineficacia o uma vontade ngela silva a delegacao de luanda trouxe um calendario para a concretizacao de alguns passos da democratizacao e pretende sair desta ronda negocial comum a data para o cessar fogo a unita porem considera que nao esta mandatada para tal debate neste encontro