

82-CRIPT-cesar

March 5, 2018

```
In [2]: alfb = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

In [3]: texto = "Through the use of abstraction and logical reasoning, mathematics developed f

In [4]: print map(ord,[x for x in alfb])

[65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88]

In [5]: print map(chr,map(ord,[x for x in alfb]))

['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']

In [6]: from string import *
def limpiar(texto,alfb):
    L = map(ord,[x.capitalize() for x in list(texto)])
    L1 = [item for item in L if item in map(ord,[x for x in alfb])]
    C1 = join(map(chr,L1),sep = "")
    return C1

In [7]: limpiar(texto,alfb)

Out[7]: 'THROUGHTHEUSEOFABSTRACTIONANDLOGICALREASONINGMATHEMATICSDEVELOPEDFROMCOUNTINGCALCULAT
```

Cifra de César

```
In [8]: def encriptar_cesar(C,k):
    L = list(C)
    L1 = map(ord,L)
    L2 = [(item+k)%256 for item in L1]
    C1 = join(map(chr,L2),sep = "")
    return C1

In [9]: encriptar_cesar(texto,5)

Out[9]: 'Ymwtzlm%ymj%zxj%tk%fgxywfhynts%fsi%qtlnhfq%wjfxtsnsl1%rfymjrffynhx%ij{jqtuji%kwtr%htzs%

In [10]: encriptar_cesar(encriptar_cesar(texto,5),251)
```

```
Out[10]: "Through the use of abstraction and logical reasoning, mathematics developed from counting and calculation"
```

```
In [11]: encriptar_cesar(limpiar(texto, alfb), 5)
```

```
Out[11]: 'YMWTLZMLYMJZXJTKFGXYWFHYNTSFSIQTLNHFQWJFXTSNSLRFYMJRFYNHXIJ[JQTUJIKWTRHTZSYNSLHFQHZQF'
```

```
In [12]: encriptar_cesar(encriptar_cesar(limpiar(texto, alfb), 5), 251)
```

```
Out[12]: 'THROUGHTHEUSEOFABSTRACTIONANDLOGICALREASONINGMATHEMATICSDEVELOPEDFROMCOUNTINGCALCULATION'
```

Análisis de frecuencias

```
In [13]: def analisis_frec(T):  
    frecuencias = {}  
    N = len(T)  
    for letra in T:  
        if letra in frecuencias:  
            frecuencias[letra] += (1/N).n()  
        else:  
            frecuencias[letra] = (1/N).n()  
    return frecuencias
```

```
In [14]: dicc = analisis_frec(encriptar_cesar(limpiar(texto, alfb), 5)); dicc
```

```
Out[14]: {'F': 0.107212475633528,  
          'G': 0.00974658869395711,  
          'H': 0.0565302144249513,  
          'I': 0.0311890838206628,  
          'J': 0.115009746588694,  
          'K': 0.0175438596491228,  
          'L': 0.0155945419103314,  
          'M': 0.0409356725146199,  
          'N': 0.0818713450292398,  
          'O': 0.00194931773879142,  
          'P': 0.00389863547758285,  
          'Q': 0.0350877192982456,  
          'R': 0.0409356725146199,  
          'S': 0.0682261208576998,  
          'T': 0.0584795321637427,  
          'U': 0.0194931773879142,  
          'W': 0.0506822612085770,  
          'X': 0.0740740740740741,  
          'Y': 0.107212475633528,  
          'Z': 0.0233918128654971,  
          '[': 0.0136452241715400,  
          '\\': 0.00974658869395711,  
          ']': 0.00194931773879142,  
          '^': 0.0155945419103314}
```

```
In [15]: def invertir(dicc):
        dict_inv = {}
        for key in dicc:
            dict_inv[dict_inv[key]] = ord(key)
        return dict_inv
```

```
In [15]: dicc2 = invertir(dicc);dicc2
```

```
Out[15]: {0.00194931773879142: 93,
          0.00389863547758285: 80,
          0.00974658869395711: 92,
          0.0136452241715400: 91,
          0.0155945419103314: 94,
          0.0175438596491228: 75,
          0.0194931773879142: 85,
          0.0233918128654971: 90,
          0.0311890838206628: 73,
          0.0350877192982456: 81,
          0.0409356725146199: 82,
          0.0506822612085770: 87,
          0.0565302144249513: 72,
          0.0584795321637427: 84,
          0.0682261208576998: 83,
          0.0740740740740741: 88,
          0.0818713450292398: 78,
          0.107212475633528: 89,
          0.115009746588694: 74}
```

```
In [16]: L = dicc2.items();L
```

```
Out[16]: [(0.0155945419103314, 94),
          (0.0682261208576998, 83),
          (0.00194931773879142, 93),
          (0.115009746588694, 74),
          (0.0350877192982456, 81),
          (0.0136452241715400, 91),
          (0.0740740740740741, 88),
          (0.0506822612085770, 87),
          (0.0311890838206628, 73),
          (0.0565302144249513, 72),
          (0.107212475633528, 89),
          (0.0584795321637427, 84),
          (0.0233918128654971, 90),
          (0.0409356725146199, 82),
          (0.00974658869395711, 92),
          (0.0175438596491228, 75),
          (0.0194931773879142, 85),
          (0.00389863547758285, 80),
          (0.0818713450292398, 78)]
```

```
In [17]: L.sort(reverse = True);L
```

```
Out[17]: [(0.115009746588694, 74),
          (0.107212475633528, 89),
          (0.0818713450292398, 78),
          (0.0740740740740741, 88),
          (0.0682261208576998, 83),
          (0.0584795321637427, 84),
          (0.0565302144249513, 72),
          (0.0506822612085770, 87),
          (0.0409356725146199, 82),
          (0.0350877192982456, 81),
          (0.0311890838206628, 73),
          (0.0233918128654971, 90),
          (0.0194931773879142, 85),
          (0.0175438596491228, 75),
          (0.0155945419103314, 94),
          (0.0136452241715400, 91),
          (0.00974658869395711, 92),
          (0.00389863547758285, 80),
          (0.00194931773879142, 93)]
```

```
In [18]: ord('E')
```

```
Out[18]: 69
```

La letra m'as frecuente en inglés es la "E", que tiene el número 69 y le corresponde después de encriptada el número 74. Entonces la clave es el 5.

Puedes leer sobre las frecuencias de las letras en inglés en Frecuencias.