

```
In [2]: # Styling notebook
from IPython.core.display import HTML
def css_styling():
    styles = open("./styles/custom.css", "r").read()
    return HTML(styles)
css_styling()
```

Out[2]:

## Circular (rotation) substitution cypher

A substitution cypher replaces any character (or sequence of characters) by another one. The easiest are the ones that rotate characters by a certain offset. In order to deal with overflows, they just use remainders mod a given number.

In this examples we're using just lowercase characters mod 26, since this allows us to cover all 26 characters without any problems.

### Rotate character 'c' by integer n mod 26

```
In [3]: def rotN(c,n) :
        if not (c.islower()) : return c
        base = ord(c) - ord('a') # a = 0, b = 1, ...
        code = (base + n) % 26
        return chr(ord('a') + code)
```

```
In [9]: rotN('u',13) # try n = 13 ;- )
# https://en.wikipedia.org/wiki/ROT13
```

Out[9]: 'h'

```
In [5]: def rotStringN(s,n) :
        return ''.join(map(lambda c : rotN(c,n),s))
```

```
In [6]: string = 'abcdefghijklmnopqrstuvwxyz'
print(string)
print(rotStringN(string,9))

# Behold! The magic of rot13
print(rotStringN(rotStringN('hello',13),13))
```

abcdefghijklmnopqrstuvwxyz  
jklmnopqrstuvwxyzabcdefghi  
hello

## Simple letter counting class

Just counts lowercase letters, nothing else  
So, it converts the string to lowercase to begin with

```
In [7]: class Histogram :
        def __init__(self, string):
            self.freq = {} # That's a dictionary
            for c in string.lower() :
                self.incrementFreq(c)

        def incrementFreq(self,c) :
            if c.islower() :
                oldV = self.freq.get(c,None) # Lazy increment
                if oldV is None : oldV = 0
                self.freq[c] = oldV + 1
```

## Sample run with a given text (Moby Dick)

1. Rotate with an arbitrary n
2. Run statistics over the cypher string
3. Pick the most common letter
4. Assume it's an 'e' and rotate back

```
In [8]: # Original text (copied and pasted, so it looks funny)
text = 'Call me Ishmael Some years ago never mind how long precisely having littl

# Change this to play with different n values
rot = rotStringN(text,17)
print(rot)

# Run statistics
h = Histogram(rot)
l = sorted(h.freq.items(),key=lambda item: -item[1]) # Sort result descending

# l[0][0] is the character (key) in the first result tuple

# So, that's the new n to rotate back:
rotBack = ord('e') - ord(l[0][0])

# and here we go!
rotStringN(rot,rotBack)
```

```
trcc dv zjydrvc jfdv pvrij rxf evmvi dzeu yfn cfex givtzjvcp yrmzex czkkcv fi e
f dfevp ze dp glijv reu efkyzex grikztlcric kf zekvivjk dv fe jyfiv z kyflxyk z
nflcu jrzc rsflk r czkkcv reu jvv kyv nrkvp grik fw kyv nfcu zk zj r nrp z yr
mv fw uizmzex fww kyv jgcvve reu ivxlcrkzcx kyv tzitlcrkzfe nyvevmvi z wzeu dpj
vcw xifnzex xizd rsflk kyv dflky; nyvevmvi zk zj r urdg uizqqcp efmdsvi ze dp
jflc; nyvevmvi z wzeu dpjvcw zemfclerkizcp grljzcx svwfiv tfwwze nrivyfljvj reu
sizexzcx lg kyv ivri fw vmvip wlevirc z dvvk; reu vjgvtzrccp nyvevmvi dp ypgfj
xvk jlty re lggvi yreu fw dv kyrk zk ivhlzivj r jkifex dfirc gizetzgcv kf givmv
ek dv wifd uvczsvirkvcp jkvggzcx zekf kyv jkivvk reu dvkyfuztrccp beftbzcx gvfg
cv'j yrkj fww-kyve z rttflek zk yzxy kzdv kf xvk kf jvr rj jffe rj z tre kyzj z
j dp jlsjkzklkv wfi gzjkfc reu srcc nzky r gyzcfjfgyztrc wcflizjy trkf kyifnj y
zdjvcw lgfe yzj jnfiu; z hlzvkcpx krbv kf kyv jyzg kyviv zj efkyzex jligizjzcx z
e kyzj zw kyvp slk bevn zk rcdfjk rcc dve ze kyvzi uvxivv jfdv kzdv fi fkyvi ty
vizjy mvip evricp kyv jrdr wvczcxj kfnriuj kyv ftvre nzky dv
```

```
Out[8]: 'call me ishmael some years ago never mind how long precisely having little or
no money in my purse and nothing particular to interest me on shore i thought i
would sail about a little and see the watery part of the world it is a way i ha
ve of driving off the spleen and regulating the circulation whenever i find mys
elf growing grim about the mouth; whenever it is a damp drizzly november in my
soul; whenever i find myself involuntarily pausing before coffin warehouses and
bringing up the rear of every funeral i meet; and especially whenever my hypos
get such an upper hand of me that it requires a strong moral principle to preve
nt me from deliberately stepping into the street and methodically knocking peop
le's hats off--then i account it high time to get to sea as soon as i can this i
s my substitute for pistol and ball with a philosophical flourish cato throws h
imself upon his sword; i quietly take to the ship there is nothing surprising i
n this if they but knew it almost all men in their degree some time or other ch
erish very nearly the same feelings towards the ocean with me'
```

In [ ]: