Examen2015

March 4, 2018

In [23]:
```
def generador0(p):
    Generador = [i for i in xsrange(2,p)]
    L = list(factor(p-1))
    for i in xsrange (2,p):
        for item in L:
            exponente = ZZ((p-1)/item[0])
            if power_mod(i,exponente,p) == 1:
                Generador.remove(i)
                break
    return Generador
```

In [24]:
```
generador0(13)
```

Out[24]:
```
[2, 6, 7, 11]
```

In [43]:
```
def generador(p):
    L = list(factor(p-1))
    i = randint(2,p-1)
    while(1):
        for item in L:
            cont =  0
            exponente = ZZ((p-1)/item[0])
            if power_mod(i,exponente,p) == 1:
                break
            cont = cont + 1
        if cont == (len(L)-1):
            return i
        i = randint(2,p-1)
```

In [44]:
```
generador(13)
```

Out[44]:
```
7
```

In [45]:
```
def comprobar(g,p):
    L = list(factor(p-1))
    for item in L:
            exponente = ZZ((p-1)/item[0])
            if power_mod(g,exponente,p) == 1:
                return False
    return True
```

```
In [49]: comprobar(generador(nth_prime(33)),nth_prime(33))

Out[49]: True

In [73]: def clavesA():
             g = generador(next_prime(20))
             priv = randint(1,next_prime(20) - 1)
             return power_mod(g,priv,next_prime(20)),g,priv

In [112]: a,g,priv = clavesA()

In [78]: def calvesB(g):
             priv = randint(1,next_prime(20) - 1)
             return power_mod(g,priv,next_prime(20)),priv

In [113]: k,privb = calvesB(g)

In [103]: def clave():
              if power_mod(k,priv,next_prime(20)) == power_mod(a,privb,next_prime(20)):
                  return power_mod(k,priv,next_prime(20))
              return -1

In [175]: clave()

Out[175]: 6

In [194]: def claveperm(K):
              L = K.digits(base=26)
              L.reverse()
              listalfb = []
              for item in L:
                  if (item in listalfb) == False:
                      listalfb.append(item)
              if len(listalfb) < 26:
                  return "Faltan"
              return listalfb

In [200]: K = 26298398761238768123787123676834823746283476238476238476327658347568347568762398
          c = claveperm(K)

In [197]: alfb = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
          L_alfb = list(alfb)
          texto='THROUGHTHEUSEOFABSTRACTIONANDLOGICALREASONINGMATHEMATICSDEVELOPED\
          FROMCOUNTINGCALCULATIONMEASUREMENTANDTHESYSTEMATICSTUDYOFTHESHAPESANDMOT\
          IONSOFPHYSICALOBJECTSPRACTICALMATHEMATICSHASBEENAHUMANACTIVITYFORASFARBA\
          CKASWRITTENRECORDSEXISTRIGOROUSARGUMENTSFIRSTAPPEAREDINGREEKMATHEMATICSM\
          OSTNOTABLYINEUCLIDSELEMENTSMATHEMATICSDEVELOPEDATARELATIVELYSLOWPACEUNTI\
          LTHERENAISSANCEWHENMATHEMATICALINNOVATIONSINTERACTINGWITHNEWSCIENTIFICDI\
          SCOVERIESLEDTOARAPIDINCREASEINTHERATEOFMATHEMATICALDISCOVERYTHATCONTINUE\
          STOTHEPRESENTDAY'
```

```
        def ord2(c):
            return L_alfb.index(c)
        def chr2(n):
            return L_alfb[n]
```

In [199]:
```
def encriptar(texto,perm):
    L = map(ord2,texto)
    encrip = []
    for item in L:
        encrip.append(perm[item])
    fin = map(chr2,encrip)
    return fin
```

In [201]:
```
encriptar(texto,c)
```

Out[201]:
```
['G',
 'N',
 'F',
 'O',
 'I',
 'V',
 'N',
 'G',
 'N',
 'P',
 'I',
 'Z',
 'P',
 'O',
 'H',
 'U',
 'T',
 'Z',
 'G',
 'F',
 'U',
 'L',
 'G',
 'J',
 'O',
 'W',
 'U',
 'W',
 'D',
 'X',
 'O',
 'V',
 'J',
```

```
'L',
'U',
'X',
'F',
'P',
'U',
'Z',
'O',
'W',
'J',
'W',
'V',
'B',
'U',
'G',
'N',
'P',
'B',
'U',
'G',
'J',
'L',
'Z',
'D',
'P',
'Y',
'P',
'X',
'O',
'Q',
'P',
'D',
'H',
'F',
'O',
'B',
'L',
'O',
'I',
'W',
'G',
'J',
'W',
'V',
'L',
'U',
'X',
'L',
```

```
'I',
'X',
'U',
'G',
'J',
'O',
'W',
'B',
'P',
'U',
'Z',
'I',
'F',
'P',
'B',
'P',
'W',
'G',
'U',
'W',
'D',
'G',
'N',
'P',
'Z',
'S',
'Z',
'G',
'P',
'B',
'U',
'G',
'J',
'L',
'Z',
'G',
'I',
'D',
'S',
'O',
'H',
'G',
'N',
'P',
'Z',
'N',
'U',
'Q',
```

```
'P',
'Z',
'U',
'W',
'D',
'B',
'O',
'G',
'J',
'O',
'W',
'Z',
'O',
'H',
'Q',
'N',
'S',
'Z',
'J',
'L',
'U',
'X',
'O',
'T',
'K',
'P',
'L',
'G',
'Z',
'Q',
'F',
'U',
'L',
'G',
'J',
'L',
'U',
'X',
'B',
'U',
'G',
'N',
'P',
'B',
'U',
'G',
'J',
'L',
```

```
'Z',
'N',
'U',
'Z',
'T',
'P',
'P',
'W',
'U',
'N',
'I',
'B',
'U',
'W',
'U',
'L',
'G',
'J',
'Y',
'J',
'G',
'S',
'H',
'O',
'F',
'U',
'Z',
'H',
'U',
'F',
'T',
'U',
'L',
'E',
'U',
'Z',
'A',
'F',
'J',
'G',
'G',
'P',
'W',
'F',
'P',
'L',
'O',
'F',
```

```
'D',
'Z',
'P',
'C',
'J',
'Z',
'G',
'F',
'J',
'V',
'O',
'F',
'O',
'I',
'Z',
'U',
'F',
'V',
'I',
'B',
'P',
'W',
'G',
'Z',
'H',
'J',
'F',
'Z',
'G',
'U',
'Q',
'Q',
'P',
'U',
'F',
'P',
'D',
'J',
'W',
'V',
'F',
'P',
'P',
'E',
'B',
'U',
'G',
'N',
```

```
'P',
'B',
'U',
'G',
'J',
'L',
'Z',
'B',
'O',
'Z',
'G',
'W',
'O',
'G',
'U',
'T',
'X',
'S',
'J',
'W',
'P',
'I',
'L',
'X',
'J',
'D',
'Z',
'P',
'X',
'P',
'B',
'P',
'W',
'G',
'Z',
'B',
'U',
'G',
'N',
'P',
'B',
'U',
'G',
'J',
'L',
'Z',
'D',
'P',
```

```
'Y',
'P',
'X',
'O',
'Q',
'P',
'D',
'U',
'G',
'U',
'F',
'P',
'X',
'U',
'G',
'J',
'Y',
'P',
'X',
'S',
'Z',
'X',
'O',
'A',
'Q',
'U',
'L',
'P',
'I',
'W',
'G',
'J',
'X',
'G',
'N',
'P',
'F',
'P',
'W',
'U',
'J',
'Z',
'Z',
'U',
'W',
'L',
'P',
'A',
```

```
'N',
'P',
'W',
'B',
'U',
'G',
'N',
'P',
'B',
'U',
'G',
'J',
'L',
'U',
'X',
'J',
'W',
'W',
'O',
'Y',
'U',
'G',
'J',
'O',
'W',
'Z',
'J',
'W',
'G',
'P',
'F',
'U',
'L',
'G',
'J',
'W',
'V',
'A',
'J',
'G',
'N',
'W',
'P',
'A',
'Z',
'L',
'J',
'P',
```

```
'W',
'G',
'J',
'H',
'J',
'L',
'D',
'J',
'Z',
'L',
'O',
'Y',
'P',
'F',
'J',
'P',
'Z',
'X',
'P',
'D',
'G',
'O',
'U',
'F',
'U',
'Q',
'J',
'D',
'J',
'W',
'L',
'F',
'P',
'U',
'Z',
'P',
'J',
'W',
'G',
'N',
'P',
'F',
'U',
'G',
'P',
'O',
'H',
'B',
```

```
'U',
'G',
'N',
'P',
'B',
'U',
'G',
'J',
'L',
'U',
'X',
'D',
'J',
'Z',
'L',
'O',
'Y',
'P',
'F',
'S',
'G',
'N',
'U',
'G',
'L',
'O',
'W',
'G',
'J',
'W',
'I',
'P',
'Z',
'G',
'O',
'G',
'N',
'P',
'Q',
'F',
'P',
'Z',
'P',
'W',
'G',
'D',
'U',
'S']
```

```
In [206]: def desencriptar(texto,perm):
              L = map(ord2,texto)
              desencrip = []
              for item in L:
                  desencrip.append(perm.index(item))
              fin = map(chr2,desencrip)
              return fin

In [207]: desencriptar(encriptar(texto,c),c)

Out[207]: ['T',
           'H',
           'R',
           'O',
           'U',
           'G',
           'H',
           'T',
           'H',
           'E',
           'U',
           'S',
           'E',
           'O',
           'F',
           'A',
           'B',
           'S',
           'T',
           'R',
           'A',
           'C',
           'T',
           'I',
           'O',
           'N',
           'A',
           'N',
           'D',
           'L',
           'O',
           'G',
           'I',
           'C',
           'A',
           'L',
           'R',
           'E',
```

```
'A',
'S',
'O',
'N',
'I',
'N',
'G',
'M',
'A',
'T',
'H',
'E',
'M',
'A',
'T',
'I',
'C',
'S',
'D',
'E',
'V',
'E',
'L',
'O',
'P',
'E',
'D',
'F',
'R',
'O',
'M',
'C',
'O',
'U',
'N',
'T',
'I',
'N',
'G',
'C',
'A',
'L',
'C',
'U',
'L',
'A',
'T',
'I',
```

```
'O',
'N',
'M',
'E',
'A',
'S',
'U',
'R',
'E',
'M',
'E',
'N',
'T',
'A',
'N',
'D',
'T',
'H',
'E',
'S',
'Y',
'S',
'T',
'E',
'M',
'A',
'T',
'I',
'C',
'S',
'T',
'U',
'D',
'Y',
'O',
'F',
'T',
'H',
'E',
'S',
'H',
'A',
'P',
'E',
'S',
'A',
'N',
'D',
```

```
'M',
'O',
'T',
'I',
'O',
'N',
'S',
'O',
'F',
'P',
'H',
'Y',
'S',
'I',
'C',
'A',
'L',
'O',
'B',
'J',
'E',
'C',
'T',
'S',
'P',
'R',
'A',
'C',
'T',
'I',
'C',
'A',
'L',
'M',
'A',
'T',
'H',
'E',
'M',
'A',
'T',
'I',
'C',
'S',
'H',
'A',
'S',
'B',
```

```
'E',
'E',
'N',
'A',
'H',
'U',
'M',
'A',
'N',
'A',
'C',
'T',
'I',
'V',
'I',
'T',
'Y',
'F',
'O',
'R',
'A',
'S',
'F',
'A',
'R',
'B',
'A',
'C',
'K',
'A',
'S',
'W',
'R',
'I',
'T',
'T',
'E',
'N',
'R',
'E',
'C',
'O',
'R',
'D',
'S',
'E',
'X',
'I',
```

```
'S',
'T',
'R',
'I',
'G',
'O',
'R',
'O',
'U',
'S',
'A',
'R',
'G',
'U',
'M',
'E',
'N',
'T',
'S',
'F',
'I',
'R',
'S',
'T',
'A',
'P',
'P',
'E',
'A',
'R',
'E',
'D',
'I',
'N',
'G',
'R',
'E',
'E',
'K',
'M',
'A',
'T',
'H',
'E',
'M',
'A',
'T',
'I',
```

```
'C',
'S',
'M',
'O',
'S',
'T',
'N',
'O',
'T',
'A',
'B',
'L',
'Y',
'I',
'N',
'E',
'U',
'C',
'L',
'I',
'D',
'S',
'E',
'L',
'E',
'M',
'E',
'N',
'T',
'S',
'M',
'A',
'T',
'H',
'E',
'M',
'A',
'T',
'I',
'C',
'S',
'D',
'E',
'V',
'E',
'L',
'O',
'P',
```

```
'E',
'D',
'A',
'T',
'A',
'R',
'E',
'L',
'A',
'T',
'I',
'V',
'E',
'L',
'Y',
'S',
'L',
'O',
'W',
'P',
'A',
'C',
'E',
'U',
'N',
'T',
'I',
'L',
'T',
'H',
'E',
'R',
'E',
'N',
'A',
'I',
'S',
'S',
'A',
'N',
'C',
'E',
'W',
'H',
'E',
'N',
'M',
'A',
```

```
'T',
'H',
'E',
'M',
'A',
'T',
'I',
'C',
'A',
'L',
'I',
'N',
'N',
'O',
'V',
'A',
'T',
'I',
'O',
'N',
'S',
'I',
'N',
'T',
'E',
'R',
'A',
'C',
'T',
'I',
'N',
'G',
'W',
'I',
'T',
'H',
'N',
'E',
'W',
'S',
'C',
'I',
'E',
'N',
'T',
'I',
'F',
'I',
```

```
'C',
'D',
'I',
'S',
'C',
'O',
'V',
'E',
'R',
'I',
'E',
'S',
'L',
'E',
'D',
'T',
'O',
'A',
'R',
'A',
'P',
'I',
'D',
'I',
'N',
'C',
'R',
'E',
'A',
'S',
'E',
'I',
'N',
'T',
'H',
'E',
'R',
'A',
'T',
'E',
'O',
'F',
'M',
'A',
'T',
'H',
'E',
'M',
```

```
'A',
'T',
'I',
'C',
'A',
'L',
'D',
'I',
'S',
'C',
'O',
'V',
'E',
'R',
'Y',
'T',
'H',
'A',
'T',
'C',
'O',
'N',
'T',
'I',
'N',
'U',
'E',
'S',
'T',
'O',
'T',
'H',
'E',
'P',
'R',
'E',
'S',
'E',
'N',
'T',
'D',
'A',
'Y']
```