Corrigé du Devoir à la Maison n°1

Cryptage RSA

Partie A. Codage des caractères

1.

```
def Numerisation(S):
    """Code la chaine de caractères S en liste de nombres."""
    L=[]
    for s in S:
        L.append(ord(s))   # ou L=L+[ord(s)]
    return L
```

2.

```
def ConversionStr(L):
    """Convertit une liste de nombres en chaine de caractères."""
    S=""
    for x in L:
        S=S+chr(x)
    return S
```

3. On saisit dans le Shell :

```
>>> ConversionStr([66,114,97,118,111,32,33])
'Bravo !'
```

On obtient donc la chaîne de caractères `"Bravo !"`.

Partie B. Programmation du cryptage

4. On peut écrire

```
def F(a,n,c):
    return a**c%n
```

On peut aussi utiliser une fonction lambda :

```
F=lambda a,n,c:a**c%n
```

5.

```
def RSA(L,n,c):
    """Renvoie la liste des éléments de L à la puissance c modulo n."""
    M=[]
    for a in L:
        M.append(F(a,n,c))
    return M
```

6. On applique successivement les fonctions `Numerisation`, `RSA` et `conversionStr` :

```
def Cryptage(S,n,c):
    """Cryptage de S avec la clef n,c."""
    L1=Numerisation(S)
    L2=RSA(L1,n,c)
    S2=ConversionStr(L2)
    return S2
```

7.

```
>>> Cryptage("KS|o",199,7)
'Test'
```

Le cryptage de la chaîne `"KS|o"` avec la clef 7 est la chaîne de départ `"Test"`.

Ceci montre que si $c = 85$ est la clef publique alors $d = 7$ est la clef privée, permettant de décrypter.