Code RSA

par Léo Peyronnet

Décembre 2022

1 Réponses Exercices

Exercice 1
$N = 391$, $E = 151$ et $D = 7$

1. Message reçu et crypté : $C = 17$
   Soit M le message tel qu'envoyé (non crypté), alors :
   $M = C^D[N] = 17^7[391] = 204$.
2. On sait que $N = p \times q$ avec p, q deux nombres premiers. On a donc :
   $391 = p \times q = 17 \times 23$ *(résultat obtenu avec le programme cf 2.1)*
   Nous pouvons donc déduire $\varphi(N)$:
   $\varphi(N) = (p-1)(q-1) = 16 \times 22 = 352$
3. Nous connaissons la relation suivante : $E.D \equiv 1[\varphi(N)]$.
   Cette relation peut être vérifiée dans notre cas :
   $151 \times 7 \equiv 1[352] \leftrightarrow 151 \times 7[352] = 1$ *(vérifié avec le programme cf 2.1)*

Exercice 2

1. $N = 221$, $E = 11$ et $D = 35$
   (a) Soit $M = 112$ le message et C le message crypté, alors :
   $C = M^E[N] = 112^{11}[221] = 123$

2 Annexes

2.1 Programme solution de l'exercice 1

```
import math
def erathosthene(n):
    t=[]
    r=[]
    t+=[False]
    t+=[False]
    for i in range(2,n):
        t+=[True]
    for i in range(2,int(math.sqrt(n))):
        j=2*i
        while j<len(t):
            t[j]=False
            j=j+i
```

```
14      for i in range(2,n):
15          if t[i]:
16              r+=[i]
17      return r
18  def scan(tab,n):
19      for i in range(len(t)):
20          for y in range(len(t)):
21              if tab[i]*tab[y]==n:
22                  return [tab[i],tab[y]]
23      return False
24
25  e=151
26  d=7
27  n=391
28
29  print("e=",e,", d=",d,", n=",n,sep="")
30  print("=======================")
31  t=erathosthene(300)
32  t=scan(t,n)
33  print("p=",t[0]," et q=",t[1],sep="")
34  phi=(t[0]-1)*(t[1]-1)
35  print("phi(N) =",phi)
36  print("E*D%phi =",e*d%phi)
```