RSA

November 12, 2021

1 1. Cryptosystème RSA

1.1 Deux fonctions auxilliaires

[1]:
```
def bigprime(b):
  return random_prime(2^(b-1), 2^b)

def invertible(N):
  while True:
    m = ZZ.random_element(1,N);
    if gcd(m,N) == 1:
      return m
```

1.2 RSA : Initialisation

[5]:
```
def init(bit):
  global p, q, M, N, k, m, ZM;
  p = bigprime(bit)
  q = bigprime(bit); M = p * q; N = (p-1) * (q-1)
  ZM = IntegerModRing(M)
  m = invertible(N)
  k = 1/m % N
```

1.3 RSA : Codage / Décodage

[6]:
```
def code(x):
  return ZM(x)^m

def decode(x):
  return ZM(x)^k
```

1.4 RSA : Exemple

[7]:
```
init(512)
C = code(3141592653589); C
```

[7]:
```
74982326465168876686210321992725032306809927745760193022604874819805477839933663
48914349908238685380129680383034417049294670145561253641826317607744727334798710
92449619532769838654446581348377900773699839214706359944305234619686633937507607
28893094614682831750912375654501196427004937563062046921017801741987
```

[5]:
```
decode(C)
```

[5]:
```
3141592653589
```

2 2. Factorisation d'un entier / paradoxe des anniversaires

[19]:
```
# Factorisation de l'entier N
def rho(N):
  f = lambda x: (x^2+1) % N  # pas de la marche aléatoire
  a = ZZ.random_element(0,N)
  k = 1; a = f(a); b = f(a)
  while True:
    k += 1; a = f(a); b = f(f(b))  # pas simple / pas double
    d = gcd(a-b, N)
    if (d > 1):                    # collision !
      print("k = ", k, "\tk / N^(1/4) = ", k / N^(1/4).n(3))
      return([d, N/d])

init(40)
for i in range(5):
  print(rho(M), "\n")
```

```
k =  141425     k / N^(1/4) =  0.19
[427467704281, 540790564463]

k =  701191     k / N^(1/4) =  1.0
[427467704281, 540790564463]

k =  527481     k / N^(1/4) =  0.75
[540790564463, 427467704281]

k =  701191     k / N^(1/4) =  1.0
[427467704281, 540790564463]

k =  417092     k / N^(1/4) =  0.62
[540790564463, 427467704281]
```

[35]:
```
%time init(36); rho(M)
%time init(40); rho(M)
%time init(44); rho(M)
```

```
%time init(48); rho(M)
```

```
k =  61703      k / N^(1/4) =  0.38
CPU times: user 115 ms, sys: 4 ms, total: 119 ms
Wall time: 116 ms
k =  289948     k / N^(1/4) =  0.62
CPU times: user 471 ms, sys: 7 µs, total: 471 ms
Wall time: 470 ms
k =  1390790    k / N^(1/4) =  0.50
CPU times: user 2.28 s, sys: 0 ns, total: 2.28 s
Wall time: 2.28 s
k =  4745469    k / N^(1/4) =  1.0
CPU times: user 7.68 s, sys: 0 ns, total: 7.68 s
Wall time: 7.68 s
```

[35]: [112022172250031, 8907720704957]

[36]:
```
%time init(52); rho(M)
%time init(56); rho(M)
```

```
k =  13021665   k / N^(1/4) =  0.75
CPU times: user 22.5 s, sys: 3.92 ms, total: 22.5 s
Wall time: 22.5 s
k =  116043128  k / N^(1/4) =  0.88
CPU times: user 3min 24s, sys: 27.6 ms, total: 3min 24s
Wall time: 3min 24s
```

[36]: [17429714366176097, 26883669104206567]

[ ]:

[ ]: