TP 4 – Chiffrement RSA

Alice veut communiquer de manière sécurisée. Elle choisit deux nombres premiers p et q, puis calcule les produits $N = pq$ et $n = (p-1)(q-1)$. Elle choisit également un entier naturel c premier avec n puis elle publie le couple $(N\ ;\ c)$, qui est une clé publique permettant à quiconque de lui envoyer un nombre chiffré.

Les messages sont numérisés et transformés en une suite d'entiers compris entre 0 et $N-1$. Pour chiffrer un entier a de cette suite, on procède ainsi : on calcule le reste b dans la division euclidienne par N du nombre a^c, et le nombre chiffré est l'entier b.

Dans la pratique, cette méthode est sûre si on choisit des nombres premiers p et q très grands, s'écrivant avec plusieurs dizaines de chiffres. On va l'envisager ici avec des nombres plus simples : $p = 5$ et $q = 11$ (c'est-à-dire $N = 55$ et $n = 40$). Alice choisit également $c = 23$.

1. Chiffrement : Écrire une fonction algorithmique nommée **chiffrement**, prenant en argument **a**, **N** et **c** et permettant de trouver l'entier b. Faire un test avec $a = 8$.
2. Déchiffrement : dans la méthode RSA, Alice doit déterminer l'inverse de c modulo n. Elle écrit le programme ci-dessous.

```
1 def chercher exposant(c,n):
2     F=0
3     d=0
4     while F!=1:
5         d=d+1
6         F=c*d%n
7     return(d)
```

   (a) Expliquer chaque ligne du programme puis le tester pour $c = 23$ et $n = 40$.

   (b) Quelle méthode plus efficace pourrait-on utiliser pour déterminer d ?

3. Écrire une fonction ayant pour arguments **b**, **d** et **N** et retournant l'entier **a**.

Histoire

Le système RSA est appelé ainsi en l'honneur des mathématiciens **Ronald Rivest**, **Adi Shamir** et **Leonard Adleman**, qui ont inventé cette méthode de cryptage en 1977 et l'ont publiée en 1978. Il est l'un des systèmes de chiffrement les plus utilisés à travers le monde.

Sa sécurité provient du fait qu'une personne connaissant N mais ne connaissant pas la factorisation $N = pq$ est incapable de déterminer l'entier c et ne peut donc pas déchiffrer le message. Ce système est donc très robuste lorsque les entiers p et q sont grands mais pourrait tout de même être mis en défaut avec l'arrivée de l'ordinateur quantique. C'est porquoi la recherche, très active dans le domaine, s'efforce de mettre au point des systèmes dits « post quantiques ». Si certains de ces systèmes utilisent la mécanique quantique, de nombreux autres continuent de s'appuyer sur les théories arithmétiques.