Système cryptographique RSA

Un peu d'histoire

D'après le sujet de BAC Centre étrangers 2018

Le système de cryptage RSA a été inventé par les mathématiciens Ronald Rivest, Adi Shamir et Leonard Adleman en 1977 et ont publié leur travaux en 1978.

Exercice n°1

1. Cette question envisage de calculer le reste dans la division euclidienne par 55 de certaines puissances de l'entier 8.
   a. Vérifier que $8^7 \equiv 2\ (55)$.
   En déduire le reste dans la division euclidienne par 55 du nombre 8^{21}.
   b. Vérifier que $8^2 \equiv 9\ (55)$ et en déduire le reste de la division euclidienne par 55 de 8^{23}.

2. On considère l'équation (E) $23x - 40y = 1$ dont les couples $(x\,;\,y)$ d'entiers relatifs.
   a. Justifier le fait que (E) admet au moins un couple solution.
   b. Donner une solution particulière de (E).
   c. Déterminer tous les couples solutions de (E).
   d. En déduire qu'il reste un unique entier d vérifiant les conditions $0 \leqslant d < 40$ et $23d \equiv 1\ (40)$.

3. Cryptage dans le système RSA.

   Une personne A 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.
   La personne A publie le couple $(N\,;\,c)$ qui est une clé publique permettant à quiconque de lui envoyer un nombre crypté.
   Les messages sont numérisés et transformés en une suite d'entiers compris entre 0 et $N-1$.
   Pour crypter 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 crypté est l'entier b.

   Dans la pratique, cette méthode est sûre si la personne A 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 petits : $p = 5$ et $q = 11$.
   La personne A choisit également $c = 23$.

   a. Calculer les nombres N et n puis montrer que la valeur de c vérifie la condition voulue.
   b. Un émetteur souhaite envoyer à la personne A le nombre $a = 8$. Déterminer la valeur du nombre crypté b.

4. Décryptage dans le système RSA.

La personne A calcule dans un premier temps l'unique entier naturel d vérifiant les conditions $0 \leqslant d < n$ et $cd \equiv 1$ (n).

Elle garde secret ce nombre d qui lui permet, à elle seule, de décrypter les nombres qui lui ont été envoyés cryptés avec sa clé publique.

Pour décrypter un nombre crypté b, la personne A calcule le reste a dans la division euclidienne par N du nombre b^d et le nombre en clair, c'est à dire le nombre avant cryptage, est le nombre a.

On admet l'existence et l'unicité de l'entier d et le fait que le décryptage fonctionne.

Les nombres choisis par la personne A sont encore $p = 5$, $q = 11$ et $c = 23$.

a. Quelle est la valeur de d ?

b. En appliquant la règle de décryptage, retrouver le nombre en clair quand le nombre crypté est $b = 17$.

> Correction des exercices

Exercice n°1

1. a. $8^3 = 512 = 9 \times 55 + 17$ donc $8^3 \equiv 17\ (55)$.
   $8^6 = (8^3)^2 \equiv 17^2\ (55)$. Or $17^2 = 289 = 5 \times 55 + 14 \equiv 14\ (55)$.

   $8^7 = 8^6 \times 8 \equiv 14 \times 8 \equiv 2\ (55)$.
   $8^{21} = (8^7)^3 \equiv 2^3 \equiv 8\ (55)$.

   b. $8^2 = 64 \equiv 9\ (55)$.
   $8^{23} = 8^{21} \times 8^2 \equiv 8 \times 9 \equiv 17\ (55)$.
   Ainsi, le reste de la division euclidienne de 8^{23} par 55 est 17.

2. a. 23 est un nombre premier et 40 n'est pas un multiple de 23. Ces deux nombres sont donc premiers entre eux.
   D'après le théorème de Bezout, (E) admet au moins un couple solution.

   b. $40 = 1 \times 23 + 17$
   $23 = 1 \times 17 + 6$
   $17 = 2 \times 6 + 5$
   $6 = 5 \times 1 + 1$
   On remonte maintenant ces lignes :
   $1 = 6 - 5 \times 1$
   $1 = 6 - (17 - 2 \times 6) \times 1$
   $1 = 6 - 17 + 2 \times 6$
   $1 = 23 - 17 - 17 + 2 \times (23 - 17)$
   $1 = 3 \times 23 - 4 \times 17$
   $1 = 3 \times 23 - 4 \times (40 - 23)$
   $1 = 7 \times 23 - 4 \times 40$.

   Le couple $(7\,;\,4)$ est donc une solution particulière de (E).

   c. Puisque $(7\,;\,4)$ est solution tout comme $(x\,;\,y)$ on a alors $23x - 40y = 1$ et $23 \times 7 - 40 \times 4 = 1$. Par soustraction des ces deux lignes, on trouve : $23(x-7) - 40(y-4) = 0$ soit $23(x-7) = 40(y-4)$.
   23 divise donc $40(y-4)$ et les nombres 23 et 40 sont premiers entre eux.
   D'après le théorème de Gauss, 23 divise $y - 4$.
   Il existe donc un entier relatif k tel que $y - 4 = 23k$ soit $y = 23k + 4$. On trouve enfin $x = 7 + 40k$.
   Réciproquement, si $x = 7 + 40k$ et $y = 4 + 23k$ avec $k \in \mathbb{Z}$, on a $23x - 40y = 1$.
   L'ensemble des couples solutions sont donc de la forme $(7 + 40k\,;\,4 + 23k)$ avec $k \in \mathbb{Z}$.

   d. $23d \equiv 1\ (40) \Leftrightarrow 23d = 1 + 40y$ avec $y \in \mathbb{Z} \Leftrightarrow 23d - 40y = 1$ avec $y \in \mathbb{Z}$ ce qui revient au couple solution de (E).
   Pour satisfaire à $0 \leqslant d < 40$, il faut prendre $k = 0$ ce qui donne $d = 7$.

3. a. $N = pq = 5 \times 11 = 55$ et $n = (p-1)(q-1) = 4 \times 10 = 40$.

Puisque 23 et 40 sont premiers entre eux, la clé $c = 23$ fonctionne bien.

b. On cherche donc le reste dans la division euclidienne de 8^{23} par 55. D'après 1.b., ce reste $b = 17$.

4. a. Le nmobre d est l'unique entier tel que $0 \leqslant d < n$ et $cd \equiv 1\ (n)$ ce qui revient à $0 \leqslant d < 40$ et $23d \equiv 1\ (40)$. D'après la question 2.d., on a $d = 7$.

b. Le nombre crypté étant $b = 17$, le nombre en clair est le nombre a, reste de la division de b^d par N, c'est à dire le reste de la division euclidienne de 17^7 par 55.

- $17^3 = 4913 = 89 \times 55 + 18$ donc $17^3 \equiv 18\ (55)$.
- $17^6 = (17^3)^2 \equiv 18^2 \equiv 49\ (55)$
- $17^7 = 17^6 \times 17 \equiv 49 \times 17 \equiv 8\ (55)$

On en déduit que $17^7 \equiv 8\ (55)$ et comme $0 \leqslant 8 < 55$, 8 est bien le reste de 17^7 par 55.
Le nombre qui se crypte en 17 est donc bien 8.