Méthode RSA ou système RSA

Centres étrangers 11 juin 2018 Baccalauréat S
Séance du lundi 7 juin 2021 (dernier cours de mathématiques expertes de l'année scolaire 2020-2021)

On trouve des renseignements intéressants dans le cours de Thierry Sageaux sur les nombres premiers.

Le but de cet exercice est d'envisager une méthode de cryptage à clé publique d'une information numérique, appelée système RSA, 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.
Les questions 1°) et 2°) sont des questions préparatoires, la question 3°) aborde le cryptage, la question 4°) le décryptage.

1°) Déterminer le reste de la division euclidienne de 8^{23} par 55.
Il est conseillé de travailler en congruences en utilisant de petites puissances de 8.

2°) Déterminer le plus petit entier naturel *d* qui est un inverse de 23 modulo 40 (pour le produit).

3°) **Cryptage dans le système RSA**
Une personne A choisit deux nombres premiers *p* et *q* distincts, puis calcule les produits $\mathrm{N} = pq$ et $n = (p-1)(q-1)$ (*n* est l'*indicateur d'Euler* de N).
Elle choisit également un entier naturel *c* premier avec *n*.
La personne A publie le couple $(\mathrm{N}\,;c)$, 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 naturels compris entre 0 et $\mathrm{N}-1$.
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 simples : $p=5$ et $q=11$.
La personne A choisit également $c=23$.
a) Calculer les nombres N et *n*, puis justifier que la valeur de *c* vérifie la condition voulue.
On peut noter que, une fois N, *n*, *c* calculés, les nombres *p* et *q* sont ensuite détruits.
b) Un émetteur souhaite envoyer à la personne A le nombre $a=1$.
Déterminer la valeur du nombre crypté *b*.
c) 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 le plus petit entier naturel *d* tel que $cd \equiv 1$ (mod. *n*).
On notera que *d* est le plus petit entier naturel qui est un inverse de *c* modulo *n*.
Elle garde secret ce nombre *d* qui lui permet, et 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 que le décryptage ainsi décrit fonctionne.
Les nombres choisis par 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 lorsque le nombre crypté est $b=17$.
Ce résultat était-il prévisible ?
c) Déterminer le nombre en clair lorsque le nombre crypté est $b=9$.

La méthode RSA est robuste, car il est très difficile de trouver *p* et *q* à partir de N (qui est public). En effet, les algorithmes de factorisation sont très lents (de l'ordre de milliers d'années pour des entiers aussi grands), jusqu'au jour où on en trouvera de plus rapides… qui feront s'effondrer la méthode RSA telle un château de cartes.
Conclusion : La méthode RSA sera un jour abandonnée, vraisemblablement remplacée par un outil très prometteur en terme de robustesse : les courbes elliptiques (équations du type $y^2 = x^2 + ax + b$). Il semble que leur résistance soit vraiment démentielle (mais là, on entre dans le domaine terriblement complexe de la géométrie algébrique…).

Corrigé

1°) Il y a plusieurs manières de faire.
La plus grande puissance de 8 calculable sur la calculatrice est 8^{11}.
Le reste de la division euclidienne de 8^{11} par 55 est 52.
On peut donc écrire $8^{11} \equiv -3$ (mod. 55) donc $8^{22} \equiv 9$ (mod. 55). On a alors $8^{22} \times 8 \equiv 9 \times 8$ (mod. 55) soit $8^{23} \equiv 72$ (mod. 55) soit $8^{23} \equiv 17$ (mod. 55).

2°) Il s'agit de déterminer le plus petit entier naturel d tel que le reste de la division euclidienne de $23d$ par 40 soit égal à 1.

Il y a plusieurs méthodes de résolution.

1ère méthode :
On utilise la calculatrice.
On rentre la fonction Y1 = reste(23X,40.
On trouve $d = 7$.

2e méthode :
On utilise une équation diophantienne.

3°)
p et q : nombres premiers distincts
$N = pq$
$n = (p-1)(q-1)$
c premier avec n
clé $= (N ; c)$
$p = 5$
$q = 11$
$c = 23$

a) $N = 55$
$n = 40$

23 est un nombre premier. Comme 23 ne divise pas 40, 23 est premier avec 40.
Autrement dit, c et n sont premiers entre eux.

b) $a^c = 1$
b est le reste de la division euclidienne de 1 par 55.
Donc $b = 1$.

c) b est le reste de la division euclidienne de 8^{23} par 55.
On en déduit que $b = 17$.

4°)
a) $cd \equiv 1$ (mod. n) soit $23d \equiv 1$ (mod. 40).
D'après le résultat de la question 2°), on a $d = 7$.

b) En appliquant la règle de décryptage, retrouver le nombre en clair lorsque le nombre crypté est $b = 17$.
Ce résultat était-il prévisible ?

$b^d = 17^7$
On cherche le reste de la division euclidienne de 17^7 par 55.
Grâce à la commande de la calculatrice, on trouve 8.
Ainsi, $a = 8$.
Le résultat était prévisible.

c) On cherche le reste de la division euclidienne de 9^7 par 55.
Grâce à la commande de la calculatrice, on trouve 4.
Ainsi, $a = 4$.