Cryptage RSA

Inspiré du sujet 019 Voir commentaires en fin de document.

Exercice 1

Alice désire transmettre à Bob une chaîne de caractères confidentiels. Elle souhaite pour ce faire utiliser un système de cryptage à clés publiques et privées. Ils disposent tout deux d'un tableur.

1. Illustrer brièvement le principe du cryptage RSA.
2. Créer une feuille de calculs permettant à Alice de crypter la chaîne de caractère « **3dX7wtt7** » (attention la casse importe)
3. Créer une seconde feuille de calcul permettant à Bob de décrypter le message que lui a transmis Alice

---

Correction

1. La méthode de cryptage dite RSA fut mise au point par les mathématiciens par Ron Rivest, Adi Shamir et Len Adleman en 1977, c'est une méthode dite à clé publique.

   Illustration de son principe de fonctionnement.

   Alice choisit deux « grands » nombres premiers p et q que seuls elle et Bob devront connaître.
   On calcule $N = pq$ qui est diffusé, c'est la première clé publique.
   Alice choisit un entier e premier avec $(p-1)(q-1)$, c'est la seconde clé publique.
   Alice peut maintenant crypter le nombre M en calculant M^e modulo N et le transmettre à Bob.
   De son côté Bob peut décrypter le message reçu, en déterminant un entier d tel que $ed \equiv 1[(p-1)(q-1)]$, ainsi en calculant $(M^e)^d$ modulo N, il retrouve M.

2. Pour réaliser les feuilles de calculs on utilise OpenCalc, tableur de la suite bureautique libre OpenOffice. (Télécharger le fichier tableur `http://akbida.free.fr/ressources/epreuve_pratique/sujet019.ods`).

   (a) On choisit deux « grands » nombres premiers $p = 37$ et $q = 13$, on a $N = pq = 481$.
   On calcule $(p-1)(q-1) = 36 \times 12 = 432$, on choisit $e = 7$ qui est premier avec 432.

   (b) On va tout d'abord transformer la chaîne de caractère en utilisant le code ASCII
   On peut générer un tableau de conversion en utilisant la fonction **=CAR()** qui, à un nombre compris entre 1 et 126 associe le caractère ASCII correspondant (cf 3^e feuille de calculs).
   Il existe une autre fonction **=CODE()** qui associe à un caractère son code mais il s'agit du code de la table de caractère active qui n'est pas général le code ASCII.

	A	B	C	D	E	F	G	H	I
1	Caractère	3	d	X	7	w	t	t	7
2	Code ASCII	051	100	088	055	119	116	116	055
3	Clé publique N	481							
4	Clé publique e	7							

   La chaîne de caractère « 3dX7wtt7 » est encodé de la manière suivante
   051 100 088 055 119 116 116 055, c'est cette chaîne que l'on va crypter.

   (c) Pour le cryptage, on peut travailler par blocs de trois chiffres car tous les blocs sont inférieurs à 481.
   Il faut calculer :
   051^7 modulo 481 100^7 modulo 481 ..... 055^7 modulo 481

   On peut directement calculer **=MOD(B3^B4 ;B3)**, car avec $e = 7$ on reste dans les limites du tableur. Mais pour pouvoir généraliser, il est préférable d'utiliser la décomposition de 7 en base de 2. (Astuce : on obtient la décompostion en base 2 d'un nombre N avec **=BASE(N ;2)**.)
   On a $51^7 = 51^{2^2+2^1+2^0} = 51^{2^2} \times 51^{2^1} \times 51^{2^0}$, ce qui permettra de calculer de manière récursive les congruences modulo 481.

	A	B	C	D	E	F	G	H	I
1	Caractère	3	d	x	7	w	t	t	7
2	Code ASCII	051	100	088	055	119	116	116	055
3	Clé publique N	481							
4	Clé publique e	7							
5									
6	2 ^0	051	100	088	055	119	116	116	055
7	2 ^1	196	380	048	139	212	469	469	139
8	2 ^2	417	100	380	081	211	144	144	081
9	Code crypté	467	100	023	198	362	129	129	198

Dans la cellule **B6** on saisit **=B2**.

Dans la cellule **B7** on saisit **=MOD(B$6^2;$B$3)** et on eétend la formule à la cellule **B8**

Il reste à calculer le produit, dans la cellule **B9** on saisit **=MOD(PRODUIT(B$6 :B$8);B3)**

On sélectionne les cellules de **B6** à **B9** et on étire les formules vers la droite jusqu'à la colonne **I**

La chaîne est maintenant cryptée 467 100 023 198 362 129 129 198, on la transmettre à Bob.

3. Phase de décryptage pour Bob.

   (a) Il faut tout d'abord déterminer l'inverse de $e = 7$ modulo $(p-1)(q-1) = 432$.

   On peut utiliser l'identidé de Bezout puisque 7 est premier avec 432. Il faut déterminer les entiers u et v tels que $u \times 432 + v \times 7 = 1$, on utilise l'algorithme d'Euclide :

$$\begin{aligned} 432 &= 7 \times 61 + 5 \\ 7 &= 5 \times 1 + 2 \\ 5 &= 2 \times 2 + 1 \end{aligned}$$

   Il suffit de « remonter » l'algorithme

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ 1 &= 432 - 7 \times 61 - (7 - 5) \times 2 \\ 1 &= 432 - 7 \times 61 - 7 \times 2 + 5 \times 2 \\ 1 &= 432 - 7 \times 61 - 7 \times 2 + (432 - 7 \times 61) \times 2 \\ 1 &= 3 \times 432 - 185 \times 7 \end{aligned}$$

   d'où $-185 \times 7 \equiv 1[432]$ on utilisera $d = 432 - 185 = 247$ comme inverse de 7 modulo 432.

   On aura besoin de la décomposition de 247 en base 2, $247 = 2^7 + 2^6 + 2^5 + 2^4 + 0 \times 2^3 + 2^2 + 2^1 + 2^0$.

   (b) Dans une deuxième feuille de calcul, on prépare la phase de décryptage.

	A	B	C	D	E	F	G	H	I
1	Code ascii crypté	051	100	088	055	119	116	116	055
2	Clé publique N	481							
3	Clé privée	247							
4									
5	2 ^0	467	404	23	198	362	129	129	198
6	2 ^1	196	157	48	243	212	287	287	243
7	2 ^2	417	118	380	367	211	118	118	367
8	2 ^3	248	456	100	9	269	456	456	9
9	2 ^4	417	144	380	81	211	144	144	81
10	2 ^5	248	53	100	308	269	53	53	308
11	2 ^6	417	404	380	107	211	404	404	107
12	2 ^7	248	157	100	386	269	157	157	386
13	Code ascii décrypté	467	100	023	198	362	129	129	198
14	Caractère	3	d	x	7	w	t	t	7

Dans la cellule **B1** on fait référence au code ASCII crypté de la feuille précédente **='Nomdelafeuille'.B9**, on étire vers la droite jusqu'à la cellule **I1**.

Pour décrypter, on utilise le même procédé que dans la question 2.

Dans la cellule **B5** on saisit **=B1**,

puis en **B6** on saisit **=MOD(B$5 ;$B$2)** on étire vers le bas jusqu'à la cellule **B12**.

Ensuite on sélectionne les cellules de **B5** à **B12** que l'on étire vers la droite jusqu'à la colonne **I**.

Il reste à saisir dans la cellule **B13**, **=MOD(B5*B6*B7*B9*B10*B11*B12 ;B2)** (le produit n' inclut pas la cellule B8 car $247 = 11\,110\,111$ en base 2), formule que l'on étire vers la droite jusqu'à la cellule **I13**.

Pour finir le décryptage, dans la cellule **B14**, il faut convertir le code ASCII en caractére, on saisit **=CAR(B13)** et on étire vers la droite jusqu'à la cellule **I14**.

La chaîne est ainsi décryptée.

Commentaires

Il s'agit d'un sujet très intéressant plutôt de type TPE. Il est difficile à aborder pour des élèves de terminales dans le cadre d'un examen en temps limité. Tant au niveau de la théorie que de la mise en place pratique à l'aide d'un tableur. On se demande pourquoi préconiser l'utilisation du tableur tant il est inadapté, on s'oblige à des restrictions pour les choix des deux nombres premiers p et q et à des astuces pour calculer les puissances M^e modulo N. L'usage d'un logiciel de calcul formel tel que xmaxima serait plus heureux en effet, xmaxima calcule sans limitation (sauf celle du temps) avec les nombres entiers. On aurait pu aussi sugérer l'usage d'un langage de programmation tel que Python dont la syntaxe est simple et est très adapté aux calculs avec les entiers.