Le chiffrement RSA

Tearii CRIDLAND.

Référence utilisée :
"Panorama des mathématiques du supérieur" (PMS),
disponible aux éditions Ellipses.

Définition 1: $\forall (a,b,n) \in \mathbb{Z}^3$, on dit que a est **congru** à b modulo n s'il existe $k \in \mathbb{Z}$ tel que $a = kn+b$ et on note alors $a \equiv b[n]$.

Exemple 1: La partie entière de $225/7$ est 32 et $225-32\times 7 = 1$ donc $225 \equiv 1[7]$, on a aussi $225 \equiv 8[7]$ en ajoutant 7 ou $225 \equiv -6[7]$ en retranchant 7.

Propriété 1: $\forall (a,b,a',b',n) \in \mathbb{Z}^5$, $(a \equiv b[n]$ et $a' \equiv b'[n]) \implies (a+a' \equiv b+b'[n]$ et $aa' \equiv bb'[n])$.

Preuve : On note $(k,k') \in \mathbb{Z}^2$ tels que $a = kn+b$ et $a' = k'n+b'$ et on a $a+a' = (k+k')n+(b+b')$ et $aa' = (kn+b)(k'n+b') = kk'n^2+knb'+k'nb+bb' = (kk'n+kb'+k'b)n+bb'$ d'où la conclusion.

Remarque 1: La relation de congruence est dite compatible avec l'addition et la multiplication.

Théorème 1: (Fermat) $\forall p \in \mathbb{P}, \forall n \in \mathbb{N}$, si p ne divise pas n alors $n^{p-1} \equiv 1[p]$.

Preuve : On note $\mathcal{P}_n$ la proposition "$n^p \equiv n[p]$" que l'on démontre par récurrence, il est clair que la proposition $\mathcal{P}_1$ est vraie, supposons pour $n \in \mathbb{N}$ que $\mathcal{P}_n$ est vraie, d'après la formule du binôme de Newton on sait que $(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^k = 1+n^p+\sum_{k=1}^{p-1}\binom{p}{k}$, de plus pour $k \in [\![1, p-1]\!]$ on remarque que $\binom{p}{k} = p \times \frac{(p-1)!}{(p-k)!k!}$ où $\frac{(p-1)!}{(p-k)!k!}$ est un nombre entier ce qui signifie que p divise $\binom{p}{k}$, en effet k est premier avec p donc $k!$ est aussi premier avec p d'après le corollaire [1] du théorème de Bézout puis $k!$ divise $\frac{(p-1)!}{(p-k)!}$ d'après le théorème [2] de Gauss ce qui prouve bien que $\frac{(p-1)!}{(p-k)!k!}$ est un nombre entier, comme $\binom{p}{k}$ est un multiple de p on a $(n+1)^p \equiv n^p+1[p]$ puis $(n+1)^p \equiv n+1[p]$ en utilisant l'hypothèse de récurrence $\mathcal{P}_n$ ainsi on obtient $\mathcal{P}_{n+1}$ et la récurrence est achevée, on vient de montrer que $n^p \equiv n[p]$ c'est à dire que $\exists k \in \mathbb{Z}$ tel que $n^p = kp+n$, puisque n divise n^p-n il divise kp mais comme n est premier avec p on sait que n divise k d'après le théorème de Gauss, finalement en divisant la dernière égalité par n on obtient $n^{p-1} \equiv 1[p]$.

Propriété 2: (Chiffrement RSA) Soit $(p,q) \in \mathbb{P}^2$ tels que $p \neq q$, si on note $n = pq$ et $N = (p-1)(q-1)$ et que l'on considère $(c,d) \in \mathbb{N}^2$ tels que $cd \equiv 1[N]$ alors on a $\forall m \in \mathbb{N}, m^{cd} \equiv m[n]$.

Preuve : Si p divise m alors on a $m \equiv 0[p]$ et $m^{cd} \equiv 0[p]$ d'après la propriété 1 donc $m^{cd} \equiv m[p]$, montrons que cela reste valable lorsque p ne divise pas m, d'après le théorème 1 on sait que $m^{p-1} \equiv 1[p]$ donc on a $(m^{p-1})^{q-1} \equiv 1^{q-1}[p]$ d'après la propriété 1 c'est à dire $m^N \equiv 1[p]$, par hypothèse $\exists k \in \mathbb{N}$ tel que $cd = kN+1$ et on a $m^{kN} \equiv 1[p]$ puis $m^{kN+1} \equiv m[p]$ d'après la propriété 1, ceci montre que $m^{cd} \equiv m[p]$ et on peut reprendre le même raisonnement avec q pour vérifier aussi que l'on a $m^{cd} \equiv m[q]$, finalement $\exists (\alpha,\beta) \in \mathbb{Z}^2$ tels que $m^{cd}-m = \alpha p = \beta q$ et d'après le théorème de Gauss on a p qui divise β donc $m^{cd}-m \equiv 0[pq]$ ce qui nous donne bien $m^{cd} \equiv m[n]$.

Définition 2: Dans la propriété précédente, on dit que le couple (n,c) est la **clé de chiffrement** et que le couple (n,d) est la **clé de déchiffrement**.

Exemple 2: On choisit pour clé de chiffrement $(n,c) = (4307,5)$, comment peut-on chiffrer la 19-ème lettre de l'alphabet "s" ? Il suffit de chiffrer le message $m = 19$ donc de déterminer un nombre congru à m^c modulo n, la partie entière de $m^c/n = 19^5/4307$ est 574 et on a $19^5 - 4307 \times 574 = 3881$, ainsi un chiffrement possible de la lettre "s" est 3881. Comment peut-on retrouver le message si l'on dispose de la clé de déchiffrement $(n,d) = (4307,3341)$? On recherche un nombre congru à $m^{cd} = 3881^{3341}$ modulo n, la partie entière de $3881^{3341}/4307$ est difficile à obtenir avec une calculatrice car le nombre est trop grand, on peut toutefois décomposer l'exposant 3341 en utilisant des multiplications et des additions de chiffres $3341 = ((5\times 3+2)\times 3+2)\times 7\times 3\times 3+2$ ce qui permet ensuite de procéder de proche en proche en utilisant la propriété 1.

1. PMS : I.C.3.e.2. 2. PMS : I.C.3.f.1.

Voici les congruences modulo 4307 obtenues ainsi permettant de trouver un nombre congru à 3881^{3341} :

- $3881^2 \equiv 582$
- $3881^3 \equiv 1874$
- $3881^5 \equiv 582 \times 1874 \equiv 997$
- $3881^{15} \equiv 997^3 \equiv 3501$
- $3881^{17} \equiv 3501 \times 582 \equiv 371$
- $3881^{51} \equiv 371^3 \equiv 1019$
- $3881^{53} \equiv 1019 \times 582 \equiv 2999$
- $3881^{371} \equiv 2999^7 \equiv 1149$
- $3881^{1113} \equiv 1149^3 \equiv 2777$
- $3881^{3339} \equiv 2777^3 \equiv 3604$
- $3881^{3341} \equiv 3604 \times 582 \equiv 19$

La clé de déchiffrement $(n, d) = (4307, 3341)$ nous a donc bien permis de retrouver le message d'origine : la 19-ème lettre de l'alphabet c'est à dire "s".

Supposons que l'on est au courant que le système de chiffrement RSA est utilisé et que l'on nous donne même la clé de chiffrement, pouvait-on deviner la clé de déchiffrement à partir de la clé de chiffrement ? Il s'agit de déterminer d à partir de c mais la seule information que nous possédons est que d est l'inverse de c modulo N c'est à dire que d vérifie la relation $cd \equiv 1[N]$. Il faudrait ainsi connaître $N = (p-1)(q-1)$ donc la décomposition en facteurs premiers de n, comme n n'est pas trop grand dans cet exemple on peut utiliser une calculatrice pour trouver $n = pq = 59 \times 73$ puis $N = 58 \times 72 = 4176$. La relation à étudier est ainsi $5d \equiv 1[4176]$, cette relation implique qu'il existe $k \in \mathbb{Z}$ tel que $5d + 4176k = 1$, il s'agit d'une identité de Bézout dont les coefficients (d, k) peuvent être déterminés en calculant le plus grand diviseur commun de 5 et 4176 par l'algorithme d'Euclide, ce nombre est $5 \wedge 4176 = 1$ et une division euclidienne donne $4176 - 835 \times 5 = 1$ donc $5 \times (-835) \equiv 1[4176]$, en additionnant la congruence $5 \times 4176 \equiv 0[4176]$ on déduit que $5 \times 3341 \equiv 1[4176]$ ce qui nous permet bien de conclure que $d = 3341$.

Remarque 2: On constate avec cet exemple que pour trouver la clé déchiffrement à partir de la clé de chiffrement il faut réussir dans un premier temps à trouver la décomposition en facteurs premiers de $n = pq$, cette décomposition est difficile à déterminer même en utilisant un puissant ordinateur lorsque les deux nombres premiers p et q sont très grands. Cette difficulté de calcul assure la qualité et la solidité du chiffrement RSA.