Principe du chiffrement RSA

Une personne, Alice, cherche à recevoir des messages de manière sécurisée et une personne, Bob, cherche à lui en envoyer. Les messages sont transformés en une suite d'entiers de telle sorte que l'objectif est de transmettre des entiers sans que quiconque, autre qu'Alice, puisse les décrypter.
Pour cela, Alice 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 e premier avec n. Alice publie le couple $(N; e)$, appelé **clé publique**, permettant à quiconque de lui envoyer un nombre crypté.

1. Pour crypter un entier m compris entre 0 et $N-1$, Bob calcule le reste c dans la division euclidienne de m^e par N. Le nombre crypté qu'il envoie à Alice est c.
2. Pour décrypter le message envoyé par Bob, Alice doit connaître l'unique entier d, appelé **clé privée**, compris entre 0 et $n-1$ tel que $ed \equiv 1[n]$. Il est alors possible de montrer que cet entier d vérifie $c^d \equiv m[N]$, ce qui permet donc à Alice de retrouver le nombre m.

Mise en œuvre de l'algorithme sur un exemple

Exercice 1. On met en œuvre l'algorithme de cryptage et de décryptage du système RSA dans le cas où $p = 5$, $q = 11$ (c'est-à-dire $N = 55$ et $n = 40$) et $e = 23$.

1. Bob veut crypter le nombre $m = 3$. Quelle est la valeur de l'entier c que Bob doit transmettre à Alice ?
2. Vérifier que l'entier $d = 7$ est tel que $ed \equiv 1[n]$.
3. Vérifier qu'Alice va bien retrouver la valeur de m, si elle reçoit la valeur c transmise par Bob.

Exercice 2. Alice communique sa clé publique au monde entier : $N = 85$ et $e = 5$.

1. Bob veut envoyer le message $m = 10$ à Alice. Quel message envoie-t-il à Alice ?
2. Alice reçoit le message $c = 40$ chiffré par Bob, elle le décrypte à l'aide de sa clé privée 13. Vérifier qu'elle retrouve bien le message initial.

Exercice 3. Cette fois Alice prend $p = 7$, $q = 13$ et $e = 5$.

1. Quelle est la clef publique ? Quelle est la clef secrète ?
2. On suppose que le message à coder est $m = 18$, quel est le message chiffré correspondant ?
3. Si Alice reçoit le message chiffré $c = 6$, quel est le message clair ?
4. Même question si $c = 1$.

Mauvaises utilisations de RSA

Exercice 4. Soit un système à clé publique utilisant le RSA, vous interceptez le texte chiffré $c = 10$ envoyé par un utilisateur dont la clé publique est $e = 5$ et $N = 35$. Que vaut m ?

Exercice 5. On note (n,e) la clé publique d'un système RSA.

1. Si $N = 35$ déterminer tous les e possibles.
2. Si $N = 211 \times 499$ peut-on prendre $e = 1623$?
3. Si la clé publique est $(492153, 2237)$, quelle est la clé privée ?

4. Même question avec $(52173, 361)$. Lequel de ces deux choix de clé privé est le plus judicieux? Que doit-on éviter dans les choix de p et q?

Exercice 6.
- Bob et Ted utilisent les mêmes nombres premier p et q, et donc le même N, mais avec des exposants e_1 et e_2 différents.
- e_1 et e_2 sont premiers entre eux.
- Alice envoie le même message m à Bob et à Ted.
- Charlie intercepte les 2 messages.

Charlie peut retrouver m. Comment?

Exercice 7. Exposant e trop petit
- Alice envoie un message m à trois personnes : Bob, Ted et Fred.
- Les clés publiques de Bob, Ted et Fred sont respectivement $N_1 = 85$, $N_2 = 143$, $N_3 = 133$ avec $e = 3$ et $m < N_i$ avec $i \in 1,2,3$.
- Charlie intercepte les 3 messages.
  - 73 pour Bob,
  - 90 pour Ted,
  - 125 pour Fred,

Charlie peut retrouver m. Comment?

Aides calculatoires :
- $73 \times 143 \times 133 \times 4 + 90 \times 85 \times 133 \times 18 + 125 \times 85 \times 143 \times 110 = 190998898$
- $190998898 \equiv 238328 \bmod (85 \times 143 \times 133)$
- $62^3 = 238328$