Cryptographie avec RSA - Son fonctionnement

Par : Simon Lévesque
http://pgon.ca

Date : 2011-07-06

Contenu

Introduction....3
Ce que sont les clés publique et privée....3
La méthode RSA....4
Utilisation....5
Crypter un message....5
Décrypter un message....5
Le fonctionnement mathématique....6
Trouver le modulo N....6
Trouver les puissances e et d....6
Un exemple concret....8
Trouver le modulo N....8
Trouver les puissances e et d....8
Résultat et essaie....9

Introduction

Ce que sont les clés publique et privée

Les méthodes de cryptage les plus simples sont de simplement utiliser une fonction mathématique qui est réversible. Par exemple, vous pouvez ajouter le nombre 10 à n'importe quel nombre pour ensuite le soustraire pour retrouver le message initial. Ce sont des méthodes dites symétriques et il n'y a une seule clé qui serait dans ce cas-ci le nombre 10.

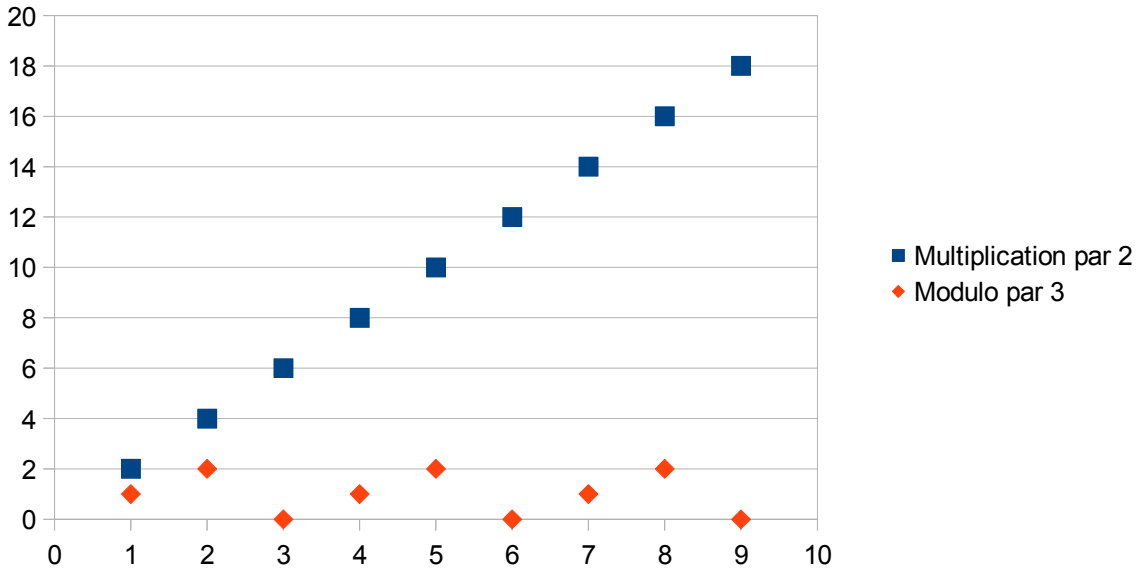
Le problème avec les clés symétriques, c'est que pour les transmettre à une autre personne, il faut passer par un canal sécurisé, sinon n'importe qui qui l'intercepte pourra décrypter les messages cryptés. Pour utiliser des services bancaires en ligne, il faudrait que la banque vous donne en main propre la clé pour s'assurer que vous êtes le seul à la connaître. S'il fallait obtenir des clés ainsi, ce serait vraiment problématique.

Le but des méthodes de cryptage avec une clé privée et une clé publique est de pouvoir s'échanger une clé sur un réseau non sécurisé. Pour ce faire, les deux clés doivent être différentes et seulement la clé publique est donnée à n'importe qui (même les personnes mal intentionnées). Ainsi, n'importe qui peut crypter des messages avec la clé publique, mais seule la personne avec la clé privée pourra décrypter. Les mots de passes peuvent alors être cryptés et seulement lus par le destinataire.

Dans le cas de la sécurisation d'un site web par HTTPS, vous comprendrez que la clé publique donnée par le site ne sert qu'à envoyer des données vers le site en question. Pour recevoir des réponses sécurisées, le navigateur va aussi transmettre une clé publique au site et garder sa clé privée. Cela crée deux canaux de communication. Par contre, pour plusieurs raisons, le protocole HTTPS n'utilise pas cette infrastructure durant toute la communication, mais ce n'est pas le propos de cet article.

La méthode RSA

Pour réussir à faire une clé asymétrique, il faut trouver une fonction qui n'est pas réversible et dont la seule façon de la craquer est par force brute. Cette façon consiste à essayer toutes les possibilités et elle doit être très longue à arriver au résultat. Par exemple, si ça prend 15 ans à décrypter votre mot de passe de compte bancaire, il se peut que vous aillez déjà fermé ce compte ou changé le mot de passe entre-temps. Cette fonction doit donner plusieurs résultats identiques, ainsi, il n'est pas possible de partir du résultat pour obtenir la valeur initiale. Par exemple, pour une multiplication par 2, la fonction inverse est la division par 2. Pour RSA, la fonction est le restant d'une division que nous appelons le modulo. Par exemple, si nous divisons 5 par 3, cela donne 1.6667, ce qui est 1 avec un restant de 2 ($1 \cdot 3 + 2 = 5$). Regardons les graphiques des deux fonctions :



Nous pouvons voir que la multiplication par 2 donne toujours une seule réponse : si nous partons de la valeur 4, le nombre initial se doit d'être 2.

Nous pouvons aussi voir que le modulo 3 va de 0 à 2 et recommence plusieurs fois. Ainsi, pour la valeur 2, nous avons une infinité de nombres initiaux possibles tels 2, 5, 8, etc. Cette fonction est donc irréversible.

Par contre, il ne suffit pas d'utiliser un modulo pour avoir une fonction cryptographique. La méthode RSA prend le message, lui ajoute une puissance définie dans la clé et à ce résultat, le modulo d'une valeur définie dans les deux clés est appliquée. De plus, cette méthode est faite pour que la fonction de cryptage soit la même que celle de décryptage. Ce qui change, c'est simplement de mettre le message crypté au lieu du message et la puissance définie dans la seconde clé (vous verrez ces équations dans la prochaine partie). Pour faire fonctionner les deux exposants avec le même modulo, le choix de toutes ces valeurs est fait en fonction de deux énormes nombres premiers avec lesquels toutes les valeurs sont calculées.

Utilisation

Crypter un message

$$Crypté = (Message)^{e} \ mod \ N$$

où

- *Crypté* est le message crypté
- *Message* est le message initial à crypter
- *e* est la puissance d'encryptage
- *mod* est le restant de la division par *N*
- *N* est la multiplication de deux nombres premiers

La clé publique contient donc les valeurs *e* et *N*.

Décrypter un message

$$Message = (Crypté)^{d} \ mod \ N$$

où

- *Message* est le message crypté une fois décrypté
- *Crypté* est le message crypté
- *d* est la puissance de décryptage
- *mod* est le restant de la division par *N*
- *N* est la multiplication de deux nombres premiers

La clé privée contient donc les valeurs *d* et *N*.

Le fonctionnement mathématique

La démarche mathématique est assez ardue pour expliquer comment trouver les valeurs de *e*, *d* et *N*, alors cette partie n'est pas montrée dans ce document. Ce que vous verrez est comment trouver les différentes valeurs utiles.

Trouver le modulo N

Pour commencer, il faut choisir deux énormes nombres premiers qui sont appelés *p* et *q*. Plus ils sont gros, plus ils seront long à trouver et à essayer lors des essais pour craquer les clés.

$$N = p \cdot q$$

L'important ici est que la grosseur maximale du message doit être inférieure à *N* puisqu'après ce nombre, il y a une boucle à cause du modulo. Par exemple, si *p* et *q* sont 3 et 5, *N* sera 15. Puis si nous voulons crypter les lettres de l'alphabet, il y a 26 lettres. Nous ne pouvons pas utiliser un *N* de 15 puisqu'il est plus petit que 26. Par contre, 5 et 7 peuvent être utilisés puisque le *N* est alors de 35.

Trouver les puissances e et d

Trouver le modulo N était assez simple à expliquer (malgré qu'il ne soit pas simple à programmer), mais pour trouver les puissances, il faut faire quelques calculs préalables.

Pour commencer, nous avons besoin d'une valeur intermédiaire *r* qui est définie comme suit :

$$r = (p-1) \cdot (q-1)$$

Ensuite, la formule qui lie *e* et *d* au modulo *N* (et en même temps aux deux nombres premiers *p* et *q*) est :

$$(e \cdot d) \, mod \, (r) = 1$$

Ce qui nous intéresse ici est de trouver la multiplication de *e* et *d* et puisqu'elle est gouvernée par un modulo, il y a plusieurs possibilités de *e* et *d*. Pour trouver toutes ces valeurs, il faut retourner à la base de ce qu'un modulo représente :

Si nous prenons un nombre *a* que nous désirons diviser par *b*, nous obtenons un quotient *q* et un restant *t*.

$$a = b \cdot q + t$$

Par exemple, le nombre 5 divisé par 3 donne un quotient de 1 et un restant de 2 :

$$5 = 3 \cdot 1 + 2$$

Si nous voulons 5 modulo 3, nous voulons savoir le restant, ce qui revient à dire :

$$a \, mod \, b = (b \cdot q + t) \, mod \, b = t$$

La partie *bq* est simplement enlevée du nombre et cela nous donne le restant. En termes plus clairs, pour trouver les valeurs de *a*, il suffit de prendre le diviseur *b*, de le multiplier par un entier *q* et d'ajouter le restant désiré. Dans notre cas,

$$(e \cdot d) \, mod \, (r) = 1$$

où

$$a = e \cdot d \; ; b = r \; ; t = 1$$

Nous avons donc

$$a = b \cdot q + t$$
$$(e \cdot d) = r \cdot q + 1$$

Et il suffit d'essayer plusieurs combinaisons de q. Il faut en essayer plusieurs puisque le nombre a d'autres contraintes :

- Le nombre ne doit pas être un nombre premier puisqu'il ne sera pas factorisable en e et d
- Les deux facteurs ne doivent pas être identiques puisque sinon la clé privée sera la même que la clé publique

Pour terminer, vous trouvez les valeurs de e et d en les factorisant.

Un exemple concret

Pour cet exemple, nous utiliserons des petits nombres premiers pour bien voir ce qui se passe et pouvoir trouver les valeurs mentalement.

Trouver le modulo N

Nous allons prendre les deux nombres premiers 3 et 5. Cela nous donne un *N* de 15.

$$p=3\,;\,q=5$$

$$N=p\cdot q$$
$$N=3\cdot 5$$
$$N=15$$

Trouver les puissances e et d

Premièrement, nous avons besoin du *r* comme suit :

$$r=(p-1)\cdot(q-1)$$
$$r=(3-1)\cdot(5-1)$$
$$r=(2)\cdot(4)$$
$$r=8$$

Deuxièmement, avec le r, nous pouvons trouver les multiples de *e* et *d* avec la formule suivante :

$$(e\cdot d)=r\cdot q+1$$
$$(e\cdot d)=8\cdot q+1$$

Voici les quelques premières valeurs possibles avec un *q* entre 1 et 6 :

q	e*d	e	d
1	9	3	3
2	17		
3	25	5	5
4	33	3	11
5	41		
6	49	7	7

Passons chacune des possibilités une à la fois :

1. Pour un *q* de 1, nous avons une multiplication de 9. Ce nombre peut être factorisé par 3 et 3. Puisque ce sont les mêmes valeurs, les clés publique et privée sont les mêmes. Ce n'est pas un bon candidat.
2. 17 est un nombre premier et ne peut pas être factorisé. Ce n'est pas un bon candidat.
3. 25 est factorisé par 5 et 5. Pour la même raison que le numéro 1, ce n'est pas un bon candidat.
4. 33 est factorisé par 3 et 11. C'est notre gagnant!
5. 41 est un nombre premier et ne peut pas être factorisé. Ce n'est pas un bon candidat.
6. 49 est factorisé par 7 et 7. Pour la même raison que le numéro 1, ce n'est pas un bon candidat.

Par conséquent, les seules bonnes valeurs dans cet échantillon sont :

$$e = 3$$
$$d = 11$$

Résultat et essaie

Pour résumer, nous avons les valeurs suivantes :

$$N = 15$$
$$e = 3$$
$$d = 11$$

Si nous voulons crypter le message qui est le nombre « 7 », il faut utiliser la formule suivante :

$$Crypté = (Message)^{e} \; mod \; N$$

$$Crypté = (7)^{3} \; mod \; 15$$
$$Crypté = 343 \; mod \; 15$$
$$Crypté = 13$$

Ensuite pour décrypter :

$$Message = (Crypté)^{d} \; mod \; N$$

$$Message = (13)^{11} \; mod \; 15$$
$$Message = 1792160394037 \; mod \; 15$$
$$Message = 7$$

Comme vous pouvez voir, nous obtenons un petit nombre « 13 » qui revient à « 7 ». Par contre, vous voyez aussi que les nombres intermédiaires sont énormes et pourtant, nous n'utilisons que des petites valeurs. Ces gros calculs font la force du cryptage, mais en même temps une faiblesse qui est le temps d'exécution. C'est pourquoi par exemple, le protocole HTTPS va utiliser le RSA au début d'une communication et ensuite envoyer une clé symétrique qui sera utilisée par la suite. Puisque la clé symétrique sera donnée par un canal sécurisé, personne ne pourra connaître la clé autre la personne désirée.

Pour terminer, voici un tableau avec quelques valeurs de message :

Message	Crypté	Décrypté	Erreur
1	1	1	
2	8	2	
3	12	3	
4	4	4	
5	5	5	
6	6	6	
7	13	7	
8	2	8	
9	9	9	
10	10	10	
11	11	11	
12	3	12	
13	7	13	
14	14	14	
15	0	0	ERREUR
16	1	1	ERREUR
17	8	2	ERREUR
18	12	3	ERREUR
19	4	4	ERREUR
20	5	5	ERREUR

Tel qu'indiqué précédemment, le message ne peut pas être plus gros que le *N*. Puisque le *N* est de 15, les messages ne peuvent être que 0 à 14.