Cryptographie Asymétrique

Yousfi Souheib

Rappel du protocole RSA

— Alice doit envoyer un message à Bob, elle a donc besoin de la clef publique RSA de Bob. Voici les différentes étapes :

1. Il choisit p et q deux grands nombres premiers (plus de 100 chiffres).
2. Il calcule n=p*q. Le nombre n, le modulo RSA, a environ 200 chiffres. Il est publique alors que p et q sont gardés secrets.
3. Il calcule $\phi(n) = (p-1)(q-1)$. qui s'appelle **la fonction d'Euler**, et qui doit rester secret. retrouver $\phi(n)$ sans connaître p et q est aussi difficile que de factoriser n
4. Il choisit un nombre e en s'assurant que $PGCD(e, \phi(n)) = 1$. Il s'agira de l'exposant de chiffrement RSA.
5. Il calcule d, inverse de e modulo $\phi(n)$ et garde secret le couple (n,d). Il s'agira de la clef privée RSA. Il la garde secrète afin de pouvoir déchiffrer par la suite le message transmis par Alice.
6. Il transmet (ou publie dans un annuaire) le couple (n,e). Ce couple s'appelle la clef publique RSA.
7. Elle convertit son message texte en un nombre M compris entre 0 et n.
8. Elle calcule $M' = M^e (mod\ n)$ et envoie ce message crypté M'.
9. Pour le décoder, il calcule $M = (M')^d (mod\ n)$ à l'aide de sa clef privée d. Ceci lui permet de retrouver le message d'origine, car : $(M')^d = (M^e)^d (mod\ n) = M^{e.d} (mod\ n) = M (mod\ n)$.
10. Il reconvertit ce nombre en un message clair.

Exercice 1

A l'aide de SageMath (https ://sagecell.sagemath.org/) et ses fonctions $is\_prime(), gcd(), ...$ Répondez à ces questions :

1. L'utilisateur A choisit les facteurs premiers $p = 11$ et $q = 23$. Trouvez n, e et d.
2. En utilisant n et e, déterminez l'espace des messages en clair 0,1,...,n-1. Puis chiffrer le message m=165 noté c.
3. En utilisant les valeurs de n, d et e déterminez à partir de c le message m.

Exercice 2

Un professeur envoie ses notes au secrétariat de votre école par email. La clef publique du professeur est (e=3,n=55=5*11), celle du secrétariat (e=3,n=33=3*11).

1. Déterminer la clef privée du professeur et celle du secrétariat de l'école. (on peut remarquer que $3 * 27 = 81 = 1 mod\ 40$ et $3 * 7 = 21 = 1 mod\ 20$.

2. Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clef RSA du secrétariat. Quel message chiffré correspond à la note 12 ?
3. Pour assurer l'authenticité de ses messages, le professeur signe chaque note avec sa clef privée et chiffre le résultat avec la clef RSA du secrétariat. Le secrétariat reçoit ainsi le message 23. Quelle est la note correspondante ?

Exemple 1

Une compagnie veut instaurer un système de commandes sur Internet. Elle instaure donc un cryptage à clef publique (RSA) pour la transmission du numéro de carte de crédit. Le numéro de carte de crédit est un numéro de 4 chiffres auquel on ajoute les 4 chiffres qui correspondent à la date d'expiration, soit un nombre de 8 chiffres.

— La compagnie choisit deux grands nombres premiers p et q.

$$next\_prime(12345) = 12347 = p$$
$$next\_prime(54589) = 54601 = q$$

— Ceci donne $n = p.q$ et $\phi(n) = (p-1)(q-1)$:

$$n = 674158547$$
$$\phi(n) = 674091600$$

— La compagnie choisit sa clef publique $e = 4559 = gcd(674091600, 4559) = 1$ et calcule son inverse $d(mod\ \phi(n)) = 227112239$.

— Un client dont le numéro de sa carte de crédit est 5678 et la date d'expiration est le 07/18 enverra donc le message $M = 56780718$.

— Le logiciel d'envoi calcule $M' = M^e(mod\ n)$=72476759.

— Le nombre M' est transmis. A la réception le logiciel de la compagnie calcule : $(M')^d mod\ n = 56780718$ qui correspond bien au numéro de la carte de crédit ainsi que sa date d'expiration.

Exemple 2

A a pris connaissance de la clef publique de B (e=3,n=253). Elle veut confirmer son rdv par lui envoyé le message 'OUI'. Elle encode O par 14, U par 20 et I par 8.

	O	U	I
M codé	14	20	08
$M' = M^3 mod\ 253$	214	157	006

Le message chiffré est donc 214 157 006.
Si A avait voulu transmettre son message M= 142008 mod 253 en un seul Bloc. Montrer en quoi cette démarche n'aurait pas permis de déchiffrer le message convenablement ?
Elle décide d'utiliser des p=5147 et q=7351. Montrer que la clef e = 307 est compatible, puis coder ce message en un bloc.
Calculer la clef de déchiffrement et vérifier le message déchiffré.