Comprendre le cryptage RSA avec . . de vrais cadenas . .

Sujet «unplugged» (sans ordinateur)

Source : http://sebsauvage.net/comprendre/encryptage/crypto_asy2.html

Prendre un coffre avec un cadenas à clé pour jouer à Alice et Bob (parfois **Bernard** en français). **Eve**, est un écouteur externe (de l'anglais *eavesdropper*), est un attaquant passif. Tandis qu'elle peut écouter les échanges d'Alice et de Bob, elle ne peut pas les modifier.

Chiffrement

Un des rôles de la clé publique est de permettre le chiffrement ; c'est donc cette clé qu'utilisera Bob pour envoyer des messages chiffrés à Alice. L'autre clé — l'information secrète — sert à *dé*chiffrer. Ainsi, Alice, et elle seule, peut prendre connaissance des messages de Bob, à condition que la brèche ne soit pas trouvée.

Alice a choisi un coffre à cadenas. Elle l'envoie ouvert à Bob, et en garde la clé. Lorsque Bob veut écrire à Alice, il y dépose son message, ferme le coffre, et le renvoie à Alice. À sa réception, seule Alice peut ouvrir le coffre, puisqu'elle seule en possède la clé, à supposer le coffre inviolable, et que personne ne puisse retrouver la clé. Voir ce que peut faire Eve contre cela.

Authentification de l'origine

D'autre part, l'utilisation par Alice de sa clé privée sur le condensat d'un message, permettra à Bob de vérifier que le message provient bien d'Alice : il appliquera la clé publique d'Alice au condensat fourni (condensat chiffré avec la clé privée d'Alice) et retrouve donc le condensat original du message. Il lui suffira de comparer le condensat ainsi obtenu et le condensat réel du message pour savoir si Alice est bien l'expéditeur. C'est donc ainsi que Bob sera rassuré sur l'origine du message reçu : il appartient bien à Alice. C'est sur ce mécanisme notamment que fonctionne la signature numérique.

Alice diffuse la clé publique du coffre et place un message dans le coffre-fort qu'elle ferme avant de l'envoyer à Bob. Si Bob parvient à l'aide de la clé publique d'Alice dont il dispose à ouvrir le coffre-fort c'est que c'est bien celui d'Alice et donc que c'est bien elle qui y a placé le message. Voir ce que peut faire Eve contre cela. Puis detailler l'authentification plus compelxe à partir de http://fr.wikipedia.org/wiki/Cryptographie_asymétrique#M.C3.A9canismes_d.27authentification

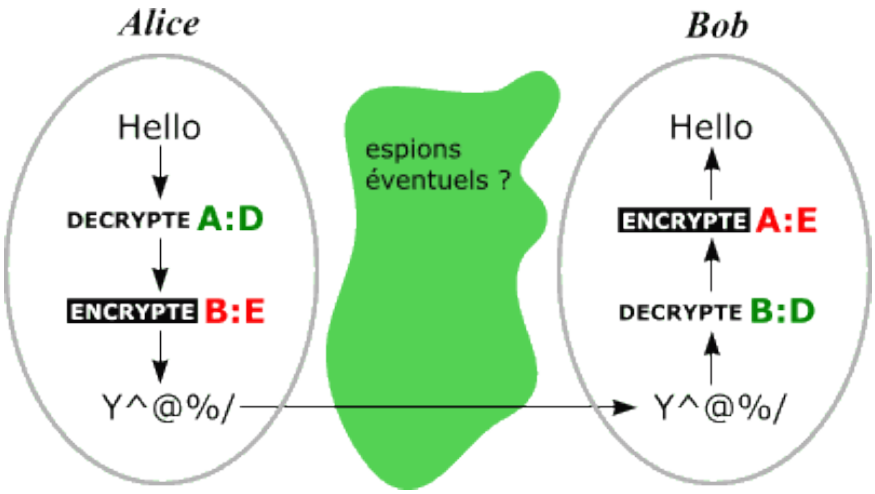
Par exemple, si Bob reçoit un message, comment peut-il être sûr qu'il provient bien d'Alice ? Quelqu'un pourrait très bien encrypter un message et l'envoyer à Bob en se faisant passer pour Alice.

Avec les algorithmes assymétriques, on peut signer un message. Soit:

- **A:E** Clé publique d'Alice (utilisée pour encrypter) donnée à tout le monde.
- **A:D** Clé privée d'Alice (utilisée pour décrypter)
- **B:E** Clé publique de Bob (utilisée pour encrypter) donnée à tout le monde.
- **B:D** Clé privée de Bob (utilisée pour décrypter)

Alice possède sa clé privée (**A:D**) et la clé publique de Bob (**B:E**).
Bob possède sa clé privée (**B:D**) et la clé publique d'Alice (**A:E**).

Quand Alice veut envoyer un message à Bob, Alice décrypte avec sa clé privée (**A:D**) pour signer le message puis l'encrypte avec la clé publique de Bob (**B:E**).



Quand Bob reçoit le message, il le décrypte avec sa clé privée (**B:D**), puis l'encrypte avec la clé publique d'Alice (**A:E**).
Si il parvient à obtenir le message en clair en **encryptant** avec la clé publique d'Alice (**A:E**), alors il est sûr que ce message vient bien d'Alice puisque Alice est la seule à posséder la clé privée correspondante (**A:D**) qui permet de **décrypter** le message.