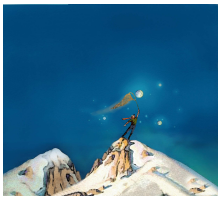

printemps des sciences
Avec le soutien de la Ministre de l'Enseignement supérieur et de la Recherche scientifique

Sciences extrêmes 19 - 25 mars 2007

SIGNATURES NUMÉRIQUES

Pokrovskaya Natalia
Département d'Informatique

Quand vous signez un papier, vous apposez dessus une marque personnelle, qui rend ce document unique et authentique et qui implique votre accord avec le contenu de ce document. Dans un ordinateur, un document est stocké sous forme numérique (une longue suite de 0 et de 1); dans ce contexte, si vous souhaitez signer un message, il n'est plus question d'utiliser un stylo. Mais comment faire alors pour signer des documents numériques?

Dans le monde de l'informatique, votre marque personnelle est une clé de chiffrement, qui vous permettra de signer un document. Pour lire vos documents, il faut utiliser une clé de déchiffrement. Ces deux clés sont un peu comme votre carte d'identité. Vous devez garder en secret votre clé de chiffrement (aussi appelée clé privée). Cette clé est unique, il n'existe normalement pas de passe-partout et personne ne peut imiter votre signature numérique (sauf en obtenant votre clé privée).
Pour permettre aux autres de lire vos documents chiffrés, vous devez leur fournir une copie de votre clé de déchiffrement (votre clé publique).

"Now we've got a joint account I won't have to forge your signature anymore."

Concrètement, la signature numérique, basée sur la cryptographie à clé asymétrique, repose sur l'exploitation d'une clé publique et d'une clé privée qui sont mathématiquement liées. L'émetteur chiffre le condensé du message (en quelque sorte le résumé de votre message) à envoyer avec l'aide de sa clé privée, et le signe grâce à une signature numérique.

En face, le destinataire peut déchiffrer la signature numérique grâce à la clé publique contenue dans un certificat électronique, accessible sur l'annuaire ou sur le site Web d'une autorité de certification. En pratique, celle-ci se présente sous la forme d'un code personnel qui permettra d'identifier avec certitude son utilisateur et d'authentifier les documents signés numériquement.

Bien plus qu'une signature manuscrite, la signature assure que le message (ou fichier) signé n'a pas été modifié depuis sa signature, si ce n'était pas le cas, il serait fort probable que quelqu'un (pas forcément vous) l'ait modifié ou qu'il y ait eu une erreur lors du transfert de ce fichier.
Imaginons que vous venez de télécharger un logiciel mais qu'un problème "invisible" soit survenu lors de la récupération du fichier; votre logiciel pourrait ne pas s'installer ou, pire, s'installer avec des fichiers corrompus (incomplets ou vérolés). Dans ce cas précis, si le fichier est signé, vous pouvez le comparer à sa signature et vous assurer qu'il n'a pas été modifié depuis sa mise en ligne ou durant le téléchargement; si la signature est invalide, cela signifie que le fichier que vous possédez sur votre disque dur ne correspond pas à celui qui a été mis en ligne et signé. Simple, non ?