Chap. 4. Signature Numérique et Fonctions de Hachage.

En pratique, on signe un haché !

§ 4.1 Signature

C'est l'un des aspects de la cryptographie asymétrique les plus utilisés, par ex : certificats numériques pour le e-commerce, signature de contrats, mise à jour de logiciels, ...

On verra le principe de la signature numérique, signature par RSA, EL.GAMAL, DSA (digital signature Standard), Courbes elliptiques.

§§ 1.1. Principe et services sécurité de la signature.

• La cryptographie asymétrique ne permet pas de traiter la distribution entre Alice et Bob ; le fait qu'1 des clés privées en crypto asymétrique permet de dire qu'un message émane de la personne ayant cette clé.