§2. Cryptographie à clé publique

(1) La cryptographie symétrique comme DES, AES, s-cryptographie, utilise la même clé pour crypter et décrypter, et l'algorithme de décryptage ressemble à celui de cryptage.

Quelques inconvénients :

- La clé le doit être partagée entre Alice et Bob en utilisant un canal sûr
- nombre de clés (et leur stockage) entre n partenaires est $\frac{n(n-1)}{2}$ assez grand.
- Impossible de traiter la non-répudiation

(2) La cryptographie à clé publique apporte des réponses à ces questions et permet aussi de traiter les points suivants :

(A) cryptage : on peut chiffrer des messages en utilisant des cryptosystèmes tels RSA, ELGAMAL, ECC, ...

(B) Etablissement de clés : sur canal non sûr (insécurisé) par ex : protocole DH, transport clé RSA.

(C) Identification : en utilisant la signature et Protocole challenge - Réponse. (typ. smart card, mobile, ...)

(D) Non-Répudiation : à l'aide de la signature

Rq : En pratique les protocoles de sécurité sont hybrides