Chap 5. Gestions de clés.

les techniques cryptographiques introduites dans les chap. précédents répondent aux 4 fonctions de sécurité citées (Chap. page). Reste quand même un point important qui est l'établissement de clés ; le protocole DH permet de répondre à cette question particulièrement.
Dans ce chap, on étudie l'établissement de clés dans les deux cas de figures (sym. et asym) et on introduit le concept important de certificats dans le cas asymétrique pour passer à l'attaque de l'homme-au-milieu.

§1. Généralités • L'établissement de clé consiste à créer des clés entre plusieurs partenaires (partage de secret). Selon les deux cas de figure :