illustre bien la cryptographie symétrique (mécanismes de diffusion, confusion). En pratique, les modes opératoires permettant l'utilisation des primitives de cryptage et décryptage. On peut très bien, par la suite introduire le protocole MAC (Passage authentification) avec le hachage (mais c'est mieux de le faire au chap. signature et hachage.)

- le chap 3. qui est fondamental étudie en détail les primitives à clé publique, illustrés par RSA, Protocole Diffie-Hellman (PDH), et une introduction aux courbes elliptiques. C'est dans ce chapitre que les éléments mathématiques sont importants: On donne juste le nécessaire (notions arithmétiques, notions de groupes, ...).
- Suite logique au chapitre 3, le chap 4. étudie la signature numérique, le hachage et le MAC. reprenant les services de sécurité cryptographique.
- le chap. 5 traite la gestion de clé (établissement, transport) et introduit la notion de certificat.