

# Chapitre 3 : Sécurité des éc

(sécurité et parallélisme)

# Plan

- Définitions
- Cryptographie symétrique
- Cryptographie asymétrique
- Infrastructures à clés publiques
- Standards de sécurité
- Annexes

# 1. Définitions

- Chiffrement = méthode visant à rendre message inintelligible par un tiers
- Déchiffrement = méthode inverse
- Cryptologie = science du chiffrement
  - Cryptographie = étude des algorithmes chiffrement et de déchiffrement
  - Cryptanalyse = étude du déchiffrement, connaître la clé

# Apports de la cryptographie

- Confidentialité
  - en rendant le contenu du message inintelligible à un tiers
- Intégrité
  - le message inintelligible ne peut pas être corrigé directement
- Authentification et non-répudiation
  - seule la source légitime a pu coder le message