Plan de l’exposé

- Définitions
  - Courbes elliptiques
  - Structure de groupe des points
  - Algorithme de multiplication rapide par addition et doublement
  - Problème du logarithme discret
- Applications
  - **Confidentialité**: Échange de clés Diffie-Hellman
  - **Authenticité**: Algorithme de Signature Digitale

Définitions

Courbe elliptique

Soient un corps $\mathbb{K}$, et des scalaires $a, b \in \mathbb{K}$, une **courbe elliptique** $\mathscr{C}$ est l'ensemble des points $(x, y) \in \mathbb{K}^2$ tels que:

$$y^2 = x^3 + ax + b$$

ainsi qu'un **point à l'infini** noté $\mathcal{O}$

Notons que la courbe est symétrique par rapport à l'axe des abscisses