Définition 0.1. *(Principe de Kerckhoffs)*
Un système de chiffrement doit être sécurisé même si tout est connu, sauf la clé.

Remarque 0.1. *Cela signifie que la sécurité ne doit pas reposer sur le secret de l'algorithme, mais uniquement sur la clé.*

L'espace des clés doit être suffisamment grand pour résister aux attaques par force brute.

On dit qu'un cryptosystème est **cassé** si un attaquant peut retrouver la clé (ou le texte clair) en un temps raisonnable.

0.1 Différents cadres d'attaques à considérer

- Un texte crypté connu
- Un texte clair connu
- Un texte clair choisi (accés à la machine de chiffrement)
- Un texte crypté choisi (accés à la machine de déchiffrement)