Agenda
Presentation plan

- Crypto refreshers

  - Definitions and security notions

  - LWE and the importance of the noise

- IND-CPA^D

  - Definitions

  - Attacks on toy schemes

Crypto refreshers