§ 2. Rappels

→ arithmétique : (thm de Fermat, Euler, ϕ, ...). 1.5

→ Groupes, Groupes cycliques.

→ classes P, NP, classes probabilistes et intérêt pour la cryptographie.

2

Nous avons délibérément suivi le cours de la réf 1). D'autres bons réf. existent on peut consulter la réf 2) ou 3) un peu plus pointues. Une fois absorbées ces bases pour l'étudiant, il peut se diriger vers plusieurs directions, notamment la cryptographie à base d'Identité (IBE : identity-Based cryptography)

→ voir les sites de la réf 1) et 2).

→ Propositions de projets.