



Master 1 de Cryptologie et Sécurité Informatique
Équipe-projet GRACE

Stage estival 2017

Rapport de stage

Étude du cryptosystème de Chor-Rivest

Rémi CLARISSE

Tuteurs : Daniel AUGOT et Luca DE FEO

Introduction

Dans l'article [1]

Références

- [1] B. Chor and R. L. Rivest. **A Knapsack-Type Public Key Cryptosystem Based on Arithmetic in Finite Fields.** *IEEE Transactions on Information Theory*, 1988.