UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENE

مكتبة سيريست
Bibliothèque CERIST

Nº D'ORDRE 05/87- M/MAT
Nº SIRC.....

U.S.T.H.B.
Service des acquisitions
Bibliothèque Universitaire

# THESE

En vue de l'obtention du
MAGISTER
En Mathématiques

Option : Algèbre et Théorie des Nombres

par

AIDER ABDELKADER

# SUJET

# Etude et estimation du coût du test de primalite de Adleman, Rumely Pomerance, Cohen et Lenstra

Soutenue le 16 Décembre 1987 devant le Jury :

| | | |
|---|---|---|
| **N. HASSANI** | Professeur à L'U.S.T.H.B. | : Président |
| **G. ROBIN** | Professeur à l'Université des Sciences de Limoges | : Rapporteur |
| **A. AINOUCHE** | Professeur à L'U.S.T.H.B. | Examinateurs |
| **B. BENZAGHOU** | Professeur à L'U.S.T.H.B. | |
| **K. BETINA** | Professeur à L'U.S.T.H.B. | |
| **M. ZITOUNI** | Professeur à L'U.S.T.H.B. | |
| **S. KONONOV** | Maître de conférence à L'U.S.T.H.B. | |

BIBLIOTHEQUE DU CERIST

# S O M M A I R E


INTRODUCTION ..... I

Chapitre 0 : Rappels de Résultats ..... 1

Chapitre I : Etude du test de primalité de ADLEMAN, POMERANCE, RUMELY, COHEN et LENSTRA .....17

1. - Introduction ..... 18

2. - Etude théorique du test d'A.P.R.C.L ..... 21

Chapitre II : Etude du coût de l'algorithme de ADLEMAN, POMERANCE, RUMELY, COHEN et LENSTRA .....74

1 - Introduction .....75

2 - Nombres $\varphi$ - intéressants .....75

3 - Estimation du coût del'algorithme d'A.P.R.C.L. .....77

3.1. Définition .....77

3.2. Choix d'un ensemble auxiliaire de nombres premiers .....77

3.3. Minoration du coût de l'algorithme d'A.P.R.C.L. .....82

Chapitre III : Programme testant les entiers naturels... 97


BIBLIOTHEQUE DU CERIST

Chapitre IV : Tables .....

- Nombres $\varphi$ - intéressants ..... I
- Nombres Euclidiens ..... IV
- Plus petits générateurs de $(\mathbb{Z}/_{q}\mathbb{Z})^{*}$, q premier inférieur à 250 ..... V
- Sommes de JACOBI ..... VI

Bibliographie.

BIBLIOTHEQUE DU CERIST