MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENE

Faculté de Mathématiques
Département d'Algèbre et Théorie des Nombres

Mémoire

Présentée pour l'obtention du diplôme de MAGISTER

En : MATHÉMATIQUES

Option : Arithmétique, Codage et Combinatoire: Algèbre et Théorie des Nombres

Sujet :

Courbes Elliptiques et Application

Présentée par : **Hafida LAIB**[(1)]

Résumé

Le domaine d'application des courbes elliptiques est très vaste. Dans ce mémoire nous allons étudier les deux problèmes de la primalité et la factorisation des grands nombres en utilisant les courbes elliptiques qui sont également utiles en cryptographie.
Nous avons présentés l'algorithme de Schoof qui permet de calculer le nombre de points d'une courbe elliptique E sur un corps fini $\mathbb{F}_q$, c'est-à-dire le cardinal du groupe $E(\mathbb{F}_q)$ où $q = p^n$.
Ensuite nous avons vu comment prouver la primalité d'un nombre avec un test de primalité en utilisant les courbes elliptiques. L'algorithme de Goldwasser-Kilian basé sur le critère de Pocklington-Lehmer est détaillé ainsi que des exemples explicites pour illustrer comment factoriser un nombre composé avec la méthode de factorisation qui a été découverte par H. W. Lenstra.
A la fin nous avons appliqués ces algorithmes avec le système algébrique SAGE.

[(1)]Directrice de mémoire : Mme. CHERCHEM Leila, Maître de Conférences A à L'USTHB.