РЕФЕРАТ

Дипломна робота складається з пояснювальної записки, обсяг якої стано-вить 51 сторінка. Структурно в роботі виділено 4 розділи.

Алгоритми факторизації поліномів необхідні в багатьої задачах крипто-логії, а також важливі для теорії кодування та вивчення лінійних рекурентних співвідношень у скінченних полях.

Метою даної роботи є розробка ефективного алгоритму факторизації полі-номів великого степеню з використанням апарату еліптичних кривих. Для цього було розглянуто теоретичні відомості про еліптичні криві (Розділ 1), існуючі алгоритми факторизації чисел та поліномів (Розділ 2), узагальнено теорему Лен-стра та розроблено, обгрунтовано і проаналізовано алгоритм факторизації поліномів над скінченним полем (Розділ 3).

АЛГОРИТМ ЛЕНСТРА, ФАКТОРИЗАЦІЯ ПОЛІНОМІВ, ФАКТОРИЗАЦІЯ ЧИСЕЛ, ЕЛІПТИЧНІ КРИВІ, СКІНЧЕННІ ПОЛЯ