АНОТАЦІЯ

Дипломну роботу виконано на 46 аркушах, вона містить 2 додатки та перелік посилань на використані джерела з 6 найменувань. У роботі наведено 8 рисунків та 1 таблиця.

Метою даної дипломної роботи є створення математичного та програмного забезпечення для асиметричної системи шифрування Меркеля-Хеллмана, та дослідження застосування LLL- алгоритму для її вдалого криптоаналізу.

У роботі було розглянуто побудову системи шифрування, що базується на NP-повній задачі про укладку ранця. Розглянуто шляхи криптоаналізу побудованої системи за допомогою LLL-алгоритму пошуку короткого базису цілочисельної решітки.

Розроблено автоматизовану систему для шифрування та розшифрування даних, також програмно реалізований її криптоаналіз. Проведення тестування розробленої системи.

Ключові слова: асиметричне шифрування,задача про укладку ранця, модульне множення, LLL-алгоритм пошуку короткого базису цілочисельної решітки.