РЕФЕРАТ

Обсяг роботи 47 сторінок, 8 рисунків, 6 таблиці, 13 літературних посилань.

Об’єктом дослідження є процеси криптографічного перетворення інформації та методи їх аналізу.

Предметом дослідження є шифр ДСТУ 7624:2014, та його стійкість до криптоаналізу методом неможливих диференціалів.

Метою даної дипломної роботи є реалізація методів пошуку неможливих диференціалі, та застосування цих методів для шифру ДСТУ 7624:2014.

Результати роботи полягають у проведенні аналізу та оцінки стійкості шифру ДСТУ 7624:2014 до атаки методом неможливих диференціалів.

КРИПТОАНАЛІЗ НЕМОЖЛИВИМИ ДИФЕРЕНЦІАЛАМИ , СЛОВО-ОРІЄНТОВНІ БЛОЧНІ ШИФРИ, SP-МЕРЕЖІ, ДСТУ 7624:2014.