РЕФЕРАТ

Обсяг роботи 76 сторінок, 6 рисунків, 4 таблиці, 26 літературних посилань. Об’єктом дослідження є реалізації аутентифікованого шифрування протоколами захищеного обміну повідомленнями. Предметом дослідження є рівень захищеності різних реалізацій аутентифікованого шифрування відносно вибору складових компонент - криптопримітивів. Метою даної дипломної роботи є дослідити різні підходи побудови аутентифікованого шифрування протоколами захищеного обміну повідомленнями та виконати їх порівняльний аналіз. Результати роботи полягають у визначенні шести напрямів для реалізації аутентифікованого шифрування програмами захищеного обміну повідомленнями, встановлення переваг та недоліків для кожного з напрямів.

ЗАГАЛЬНА КОНСТРУКЦІЯ, АУТЕНТИФІКОВАНЕ ШИФРУВАННЯ