РЕФЕРАТ

Магістерська дисертація: 94 с., 30 рис., 28 табл., 1 додаток, 24 джерел.

Актуальність. Громіздке впровадження ІТ робить актуальною проблему захисту інформації. Статистика показують, що лише деякі власники своїх фірм в цій галузі вважають свою компанію такою, яка готова протистояти сучасним інформаційним загрозам.

У цьому дослідженні вирішено питання підвищення ефективності алгоритмів шифрування та дешифрування інформації. Підвищення кількості цифрових документів та комерційних операцій створюють гостру потребу в наявності алгоритмів шифрування. Безпечні криптографічні алгоритми є дуже трудомісткими і їх ефективна реалізація необхідна для програм. У цьому дослідженні представлена паралельна реалізація та аналіз різних алгоритмів шифрування, таких як: AES (Advanced Encryption Standard), Blowfish, Twofish, DES (Data Encryption Standard), Serpent, Triple DES та RSA. Паралельна реалізація алгоритмів створена для підвищення ефективності алгоритмів. Експерименти показують, що послідовна реалізація значно поступається паралельній в часу виконанні. Алгоритми порівнюються на основі часу шифрування та дешифрування інформації та їх прискорення. Результати показують, що Triple DES є більш ефективним алгоритмом серед досліджуваних алгоритмів.

Зв'язок роботи з науковими програмами, планами, темами. Робота виконувалась на філії кафедри автоматизованих систем обробки інформації та управління Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського» в рамках теми «Розробити оптимальні за точністю та швидкодією криптографічні алгоритми, розпаралелити їх та зробити їх порівняльний аналіз».

Мета: збільшити прискорення алгоритмів шифрування та дешифрування інформації.

Для досягнення задоної мети необхідно виконати такі завдання:

– зробити огляд існуючих рішень;

– розробити алгоритми на основі існуючих засобів шифрування та дешифрування інформації, розпаралелити кожен із запропонованих алгоритмів;

– розробити програмну реалізацію поданих алгоритмів;

– здійснити порівняльний аналіз послідовного та паралельного виконання різних алгоритмів.

Об'єкт дослідження – шифрування інформації та її дешифрування.

Предмет дослідження – алгоритми за домогою яких можна здійснювати шифрування та дешифрування інформації.

Наукова новизна одержаних результатів полягає у розпаралелюванні існуючих криптографічних алгоритмів та здійсненні їх порівняльного аналізу.

Публікації. Матеріали роботи опубліковані в Міжнародній науковій конференції "iScience", в Міжнародній конференції "UKRLOGOS", у Всеукраїнській науково-практичній конференції молодих вчених та студентів "Інформаційні системи та технології управління" та в Міжнародній науковій інтернет-конференції "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення".

ЕФЕКТИВНІ МЕТОДИ ОБЧИСЛЮВАННЯ КРИПТОПРИМІТИВІВ В ПАРАЛЕЛЬНІЙ СИСТЕМІ ОБЧИСЛЕНЬ.