**Кінах Ярослав Ігорович. Методи паралельних обчислень та обгрунтування рівня криптографічного захисту інформації в комп'ютерних мережах : дис... канд. техн. наук: 05.13.13 / Тернопільський національний економічний ун-т. — Т., 2007. — 152арк. — Бібліогр.: арк. 127-137.**

|  |  |
| --- | --- |
| |  | | --- | | Кінах Я. І. Методи паралельних обчислень та обґрунтування рівня криптографічного захисту інформації в комп’ютерних мережах. – Рукопис.  Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.13 – обчислювальні машини, системи та мережі. – Тернопільський національний економічний університет, Тернопіль, 2007.  Дисертація присвячена визначенню рівня стійкості асиметричних криптоалгоритмів в комп’ютерних мережах на основі використання алгоритму ЗРЧП, що забезпечить конфіденційність та автентичність інформації. Дано рекомендації щодо вибору поліному алгоритму ЗРЧП для чисел багатократної точності різної довжини. В роботі алгоритм ЗРЧП розбито на типові алгоритмічні структури, виконано їх декомпозицію, сформульовано правила оптимізації для декомпозиції. Запропоновано засоби на основі використання розроблених правил оптимізації для обробки матриці, які суттєво зменшують час виконання цих операцій, а також час виконання алгоритму ЗРЧП, а їх реалізація підтверджує теоретичні розрахунки та адекватність запропонованих моделей. Розроблений принцип побудови оптоволоконного засобу криптоаналізу відрізняється від відомих перспективнішими часовими характеристиками, це дозволяє на практиці значно скоротити час етапу просіювання. Побудовано обчислювальну систему, що дозволяє реалізувати алгоритм ЗРЧП паралельно. Удосконалено математичну модель оцінки ефективності та прискорення виконання паралельного алгоритму. Це дозволяє скоротити час виконання криптоаналітичного алгоритму та точніше визначити рівень стійкості алгоритмів RSA та Ель - Гамала, а на практиці користуватися безпечними ключами. | |
| |  | | --- | | 1. На основі проведеного аналізу та теоретичних узагальнень встановлено, що сучасні комп’ютерні мережі є швидкісними і забезпечують високу продуктивність роботи під час обробки і збереження інформації. Проте вони потребують надійного захисту, оскільки із зростанням швидкодії мережі скорочується час виконання паралельної реалізації криптоаналітичних алгоритмів, це дає можливість несанкціонованого доступу в комп’ютерних мережах. На сьогодні задача факторизації системи RSA-2048 залишається відкритою. 2. Використовуючи метод ЗРЧП, удосконалено метод розрахунку надійності системи шифрування RSA, удосконалення полягає у:    * оптимізації етапу вибору поліному алгоритму ЗРЧП. Дослідження показали, що на практиці доцільно скористатися критерієм Ензейштейна, оскільки зменшено кількість операцій алгоритму ЗРЧП на 6%;    * скороченні часу просіювання розрідженої матриці. Запропонована інтерпретація алгоритму значно зменшує час його виконання при довільній кількості процесорів та підзадач. За такої реалізації цього етапу час його виконання зменшується у 7 разів;    * зменшенні кількості групових операцій алгоритму ЗРЧП на основі відокремлення деякого множника від елементів ідеалу, що зменшує кількість групових операцій алгоритму ЗРЧП на 5%;    * скороченні матричних операцій. Обробку матриці *Н* можна проводити без використання суперкомп’ютерів, це дозволяє проводити всі етапи криптоаналізу на персональних комп’ютерах, які під’єднані до мережі. Запропоновані удосконалення дозволяють скоротити час виконання алгоритму ЗРЧП загалом на 12%. 3. Розроблено інтегральний критерій ефективності роботи криптоаналітичної мережі, завдяки чому можна знайти оптимальні значення параметрів *ti*,*ri*, за яких досягається максимальна ефективність роботи криптоаналітичної мережі при довільних параметрах. Це дозволяє використовувати ресурси мережі у найпродуктивніший спосіб. Робота мережі є найефективнішою, для сумарної продуктивності, що дорівнює 746324с-1, а сумарний час роботи ресурсів дорівнює 3721 мксек. 4. Вперше запропоновано засоби на основі використання розроблених правил оптимізації для обробки матриці, які суттєво зменшують час виконання цих операцій, а також час виконання алгоритму ЗРЧП загалом на 24%, а їх реалізація підтверджує теоретичні розрахунки та адекватність запропонованих моделей. Розроблений принцип побудови оптоволоконного засобу криптоаналізу відрізняється від відомих перспективнішими часовими характеристиками, це дозволяє на практиці скоротити час етапу просіювання у 7 разів для ключа довжиною 768 біт. 5. В мережі доцільно використовувати ключі не менші ніж 2048 біт. Слід також синтезувати асиметричні та симетричні алгоритми з плаваючими ключами, що мають короткий життєвий цикл. Мінімальний недосяжний ключ, для запропонованої реалізації алгоритму ЗРЧП має довжину 1524 біти. | |