УДК 004.056.55

М.П. Карпінський[1], д-р. техн. наук, проф., Я.І. Кінах[2], канд. техн. наук, доц., У.О. Яциковська[1], канд. техн. наук, Р.І. Паславський[3], канд. техн. наук, доц., Т.І. Кужда[2], канд. екон. наук, доц., І. В. Бойко[2], канд. фіз.-мат. наук, доц.
[1]Академія технічно-гуманістична, Польща
[2]Тернопільський національний технічний університет імені Івана Пулюя, Україна
[3]Львівський національний аграрний університет, Україна

ЕКСПЛУАТАЦІЯ БАГАТОКОРИСТУВАЦЬКОЇ ПРОГРАМНОЇ СИСТЕМИ ДЛЯ КРИПТОАНАЛІЗУ АСИМЕТРИЧНИХ АЛГОРИТМІВ ШИФРУВАННЯ ДАНИХ

M. Karpinsky, Dr., Prof., I. Kinakh, Ph.D, Assoc. Prof., U. Yatsykovska, Ph.D, Assoc. Prof., R. Paslavsky, Ph.D, Assoc. Prof., T. Kuzhda, Ph.D, Assoc. Prof., I. Boyko, Ph.D, Assoc. Prof.

OPERATION OF MULTI-USER SOFTWARE SYSTEM FOR CRYPTOANALYSIS OF ASYMMETRIC DATA ENCRYPTION ALGORITHMS

Успіх криптоаналізу в значній мірі залежить від коректної експлуатації програмної системи. Класичні багатокористувацькі програмні системи загалом містять необхідні компоненти на робочих станціях користувачів: база даних, засоби забезпечення доступності даних для інтерфейсу додатку користувача. З цього випливає, що клієнти станції повинні надавати для самих себе весь необхідний набір сервісів і містити відповідне програмне забезпечення для криптоаналізу систем шифрування типу RSA, Ель-Гамала, еліптичних кривих. Подібна вимога значно ускладнює технічні вимоги, запропоновані до апаратної частини клієнтської робочої станції, і в остаточному підсумку призводить до ускладнення всієї системи в цілому [1].

Слід також відзначити, що подібне програмне забезпечення вимагає проведення робіт із його настроювання і підтримки цих настроювань у робочому стані. Так, користувальний додаток, що реалізує частину криптоаналітичного алгоритму повинен містити інформацію про місце його підзадачі у структурі програмної криптоаналітичної системи, дані доступу мережевого протоколу, мови бази даних, що визначає порядок алфавітного сортування й індексування. Ця робота є трудомістким процесом, особливо при великій кількості і неоднорідному парку робочих станцій на яких реалізується криптоаналіз. Відзначимо, що далеко не всі компоненти подібного програмного забезпечення інтегровано до складу дистрибутиву користувацького додатку, тому що вони є предметом ліцензування.

Очевидним є факт: чим складніша конфігурація, що забезпечує доступ до даних робочої станції, тим частіше відбуваються порушення в її роботі. Є ще один чинник, котрий пов'язаний із тим, що багато засобів розробки використовують ті самі стандартні бібліотеки доступу до даних у випадку операційної системи типу Windows це BDE і ODBC. Доцільно застосовувати екстенсивні заходи - нарощування апаратної частини робочих станцій, збільшення пропускної здатності мережі, прокладання нових ліній зв'язку, перенесення застарілих даних в архіви з метою зменшення обсягу бази даних, що звичайно вимагають чималих технічних витрат, особливо для великої кількості користувачів і високої швидкості росту обсягу бази даних під час виконання криптоаналізу. Є інші, інтенсивні методи розв'язання подібних задач. Вони можуть мати різноманітну реалізацію, але в цілому використовують одну загальну концепцію. Доцільно створювати нові програмні сервіси для користувачів програмної криптоаналітичної системи [2]. Такі сервіси, в загальному є сервісами проміжного прошарку middleware services, оскільки займають проміжний рівень між даними і сервісами, що їх обслуговують, з одного боку, і користувальними додатками,

орієнтованими на високопродуктивну обробку даних криптоаналітичного алгоритму. Ці сервіси звичайно мають мінімальний користувальний інтерфейс або не мають його зовсім. Нерідко вони можуть бути реалізовані для різноманітних платформ, тому що є сервісами більш високого рівня, ніж сервіси, специфічні для даної операційної системи. Такі сервіси можна реалізувати всередині додатків або бібліотек, так званих – Application Server, а також у вигляді служб операційних систем. Користувальні додатки, що використовують сервіси проміжного прошарку, – це клієнти.

Одним із найбільше поширених на сьогодні типів серверів додатків є сервери доступу до даних типу Data Access Server, реалізовані, як правило, у вигляді додатків рідше – у вигляді бібліотек. Їм притаманна функціональність, пов'язана з доступом до даних. Слід відзначити, що у вигляді окремого сервісу можна реалізувати не тільки доступ до даних, але і будь-яку іншу функцію користувального додатку, наприклад, обробку розріджених матриць алгоритму загального решета числового поля, генерацію бази просіювання, забезпечення коректного збору даних. У цьому випадку говорять про сервери функціональності functionality server. Сервер функціональності - більш загальне поняття, ніж сервер доступу до даних. Останній є лише окремий випадок серверу функціональності. Один сервер функціональності може в загальному випадку надавати декілька сервісів для криптоаналізу.

Особливо важливою є реалізації взаємодії між підзадачами. Слід відзначити, що ці алгоритми базуються на віддаленому виклику процедур шляхом передачі даних між об'єктами усередині клієнта й усередині сервера. Ефективним є використання stub-об'єкту, що не містить відкритої реалізації алгоритму криптоаналізу. Замість відкритої реалізації можуть присутні функції API із бібліотеки, що реалізують виклики віддалених процедур і передачу даних згенеровані утилітами. Коли перший із клієнтів, який під'єднаний до сервера, ініціював сам або за допомогою службового сервера запуск сервера, при від'єднанні всіх клієнтів сервер повинен припинити свою роботу.

Отже, для продуктивної експлуатації багатокористувацької програмної системи для криптоаналізу асиметричних алгоритмів шифрування даних доцільно використовувати технології розподілених обчисленнь. Оскільки значну частину часу процесор користувача простоює, то цей час можна використовувати для виконання обчислень, задіяти максимальну кількість техніки для роботи над задачею, тоді сукупна обчислювальна потужність такої обчислювальної системи буде достатньою для експлуатації програмної системи для криптоаналізу асиметричних алгоритмів. При проектуванні розподілених систем варто прийняти рішення про вибір конкретної технології і реалізації з урахуванням особливостей програмної розподіленої системи.

Література

1. І. З. Якименко, М. М. Касянчук, С. В. Івасьєв Криптосистема Рабіна на основі операції додавання // Математичне та комп'ютерне моделювання. Серія: Технічні науки № 19, 2019. – 145–150 с.
2. O. Yudin, R. Ziubina, S. Buchyk, O. Matviichuk-Yudina, O. Suprun, V. Development of methods for identification of information-controlling signals of unmanned aircraft complex operator / Eastern-European Journal of Enterprise Technologies // Vol 2, No 9 (104) 2019. – Pp. 56–65.