УДК 004.043
Голінський І., Твердун В. – ст. гр. СІ-41
Тернопільський національний технічний університет ім. І. Пулюя

СУЧАСНІ ВИСОКОПРОДУКТИВНІ ТА РОЗПОДІЛЕНІ ТЕХНОЛОГІЇ КРИПТОАНАЛІЗУ

Науковий керівник: к. т. н. А. М. Луцків

Криптоаналіз - наука про методи отримання вихідного значення зашифрованої інформації, не маючи доступу до секретної інформації (ключа), необхідної для цього. У більшості випадків під цим мається на увазі знаходження ключа. Під терміном «криптоаналіз» також мається на увазі спроба знайти вразливість в криптографічному алгоритмі або протоколі. Хоча основна мета залишилася незмінною з плином часу, методи криптоаналізу зазнали значних змін, еволюціонувавши від використання лише ручки і паперу до широкого застосування обчислювальних потужностей комп'ютерів у наші дні. Результати криптоаналізу конкретного шифру називають криптографічною атакою на цей шифр.

Основні методи криптоаналізу:

- Метод повного перебору (або метод «грубої сили» від англ. Brute force) - метод розв'язання задачі шляхом перебору всіх можливих варіантів.
- Метод диференціального криптоаналізу - це спроба розкриття секретного ключа блокових шифрів, які засновані на повторному застосуванні криптографічно слабкої цифрової операції шифрування n разів. При аналізі передбачається, що на кожному циклі використовується свій підключ шифрування.
- Метод «зустрічі посередині» має значно меншу трудомісткість в порівнянні з методом повного перебору, вимагає такого ж об'єму пам'яті, як метод Полларда, але при цьому піддається ефективному розпаралелюванню.
- Метод атаки по ключах передбачає перевірку в першу чергу так званих “слабких ключів”, які не забезпечують достатнього рівня захисту чи використовують в шифруванні закономірності, які можуть бути виявлені.

Складність повного перебору залежить від кількості всіх можливих розв'язків задачі. Якщо простір розв'язків дуже великий, то повний перебір може не дати результатів протягом декількох років або навіть століть. Тому корисним є реалізація паралельного виконання перебору, що значно зменшить час обробки можливих розв'язків. Для реалізації такого підходу можуть бути застосовані наступні технології:

- OpenMP (Open Multi-Processing) використовується в системах із спільною пам’яттю і реалізує паралельні обчислення за допомогою багатопоточності, в якій «головний» (master) потік створює набір підлеглих (slave) потоків і завдання розподіляється між ними. Передбачається, що потоки виконуються паралельно на машині з декількома процесорами і/або ядрами.
- Message Passing Interface (MPI, інтерфейс передачі повідомлень) - програмний інтерфейс (API) для передачі інформації, який дозволяє обмінюватися повідомленнями між процесами, які виконують одне завдання. MPI використовується для паралельних та / або розподілених обчислень.

Метою дослідження є створення системи для криптоаналізу методом повного перебору на системах зі спільною пам'яттю за допомогою OpenMP і розподіленою пам'яттю за допомогою OpenMPI, бібліотеки, яка є реалізацією стандарту MPI.