УДК 003.26.09:004.032.24:519.852.67
Напованець Р.– ст. гр. СІ-41
Тернопільський національний технічний університет імені Івана Пулюя

РОЗРОБКА РОЗПОДІЛЕНОЇ СИСТЕМИ КРИПТОАНАЛІЗУ АЛГОРИТМУ RSA

Науковий керівник: к.т.н. Луцків А.М.

Актуальність криптоаналізу асиметричних криптоалгоритмів полягає в тому, що вони використовуються для захисту каналів передачі даних у багатьох сферах життєдіяльності людини: шифрування сеансових ключів, шифрування даних, генерування цифрових електронних підписів та ін. Щоб вчасно попередити, що певний алгоритм чи деяка множина його ключів є нестійкою, для подальшого використання необхідно здійснювати дослідження його криптостійкості.

Методи криптоаналізу напряму залежать від криптоалгоритму і інформації, яку відомо про саму систему, ключі, повідомлення. Асиметричні алгоритми використовують різні ключі для шифрування та розшифрування даних, від кількості інформації, яку дано про ці ключі залежить метод атаки, який треба використовувати для криптоаналізу алгоритму. Найпоширенішими атаками на асиметричні алгоритми шифрування є: пряма атака, циклічна атака, атака методом осліплення, атака Хастада, атака по частково відомій секретній експоненті, атака Франкліна - Рейтара.

Здійснення криптоаналізу сучасних асиметричних алгоритмів шифрування є можливим за умови використання апаратних та програмних засобів високопродуктивних обчислень. Найпоширенішими за критеріями ціни, масштабовності та функціональності сьогодні є комп'ютерні системи на основі кластерних архітектур, тобто системи з розподіленою пам'яттю. Для того, щоб використовувати методи криптоаналізу на паралельних і розподілених комп'ютерних системах потрібно створювати спеціалізоване програмне забезпечення. Існує безліч технологій, які дозволяють розпаралелювати обчислення між вузлами обчислювальної системи. Для кластерних архітектур найпоширенішою парадигмою програмування є парадигма на базі обміну повідомленнями, а відповідно її реалізації: MPI (MPICH, OpenMPI) та PVM. Розробка програмного забезпечення здійснюється мовою С. Щоб спростити процес розробки криптоаналітичнго програмного забезпечення доцільно скористатися вже готовими криптографічними бібліотеками. Таких бібліотек є досить багато, одна із найпоширеніших — OpenSSL.

OpenSSL — криптографічний пакет з вільним вихідним кодом, що дає можливість легко використовувати вже готові функції і методи. Оскільки більшість мережевих протоколів, які використовуються в Інтернеті, наприклад, IMAP, POP, SQL, SMTP, HTTP, FTP, LDAP, забезпечують підтримку шифрування інформації по протоколу SSL, а OpenSSL підтримує протоколи SSL v2/v3 (Secure Sockets Layer) і TLS v1 (Transport Layer Security), то використання OpenSSL є багатофункціональним. OpenSSL одночасно зручний і практичний в роботі із всіма включеними в нього алгоритмами шифрування, тому повністю задовольняє всі вимоги роботи із асиметричними криптоалгоритмами.

В ході даного дослідження здійснюється реалізація розподіленої системи криптоаналізу асиметричного алгоритму методом прямої аткаки з використанням мови С, бібліотек і засобів паралельного програмування OpenMPI та криптографічної бібліотеки OpenSSL.