УДК 681.3.06: 519.248.681

Р. Козак, С. Прошин
(Тернопільський національний технічний університет імені Івана Пулюя)

НАПРЯМКИ РОЗВИТКУ КРИПТОАНАЛІЗУ

Останні два десятиліття характеризуються значним збільшенням кількості відкритих праць з усіх питань криптології, а криптоаналіз серед галузей досліджень, що розвиваються, займає одне з перших місць. Напрямки криптоаналізу можуть бути різноманітними, відповідно до напрямків криптографії: розкриття ключа, нав'язування хибної інформації шляхом знаходження недоліків в криптоалгоритмі чи протоколі, можливість необмеженого зчитування зашифрованої інформації тощо.

Диференціальний метод криптоаналізу запропонований Е. Біхамом і А. Шаміром в 1990 році. Диференціальний криптоаналіз – це спроба розкриття секретного ключа блочних шифрів, що ґрунтуються на повторному використанні криптографічно слабкої цифрової операції шифрування певну кількість разів. Особливістю диференціального аналізу є те, що він практично не використовує алгебраїчні властивості шифру (лінійність, афінність, транзитивність, замкнутість тощо), а побудований лише на нерівномірності розподілу ймовірності диференціалів.

Лінійний метод криптоаналізу запропонований вперше японським математиком Мацуі. Метод передбачає, що криптоаналітик знає відкриті та відповідні їм зашифровані тексти. Зазвичай для шифрування застосовується додавання по модулю 2 тексту з ключем та операції розсіювання і перемішування. У цьому випадку задача криптоаналізу – знайти найкращу лінійну апроксимацію (після усіх циклів шифрування) виразу $x_{i1} + ... + x_{ir} + y_{j1} + y_{js} = z_{kl} + ... + z_{kt}$. Результатом розвитку цього напрямку є, зокрема, можливість злому шифру DES лише із 243 відомими відкритими текстовими блоками.

Наступний напрям розвитку пов'язаний з аналізом споживаної електроенергії для розрахунку обчислення секретного ключа. Зазвичай для опрацювання логічної одиниці потрібно більше електроенергії, ніж для опрацювання логічного нуля. Якщо криптографічний алгоритм складається із цикла, в якому розряди ключа проходять почергову обробку, зловмисник, замінивши системний «гігагерцовий» системний годинник більш повільним, може з великою точністю відслідковувати потужність, споживану кожною машинною інструкцією. Запобігти злому з допомогою цього методу можна лише акуратним кодуванням алгоритму мовою Асемблера так, щоб енергоспоживання не залежало ні від спільного ключа, ані від ключів кожної ітерації.

Іще один з підходів ґрунтується на часовому аналізі. Криптографічні алгоритми містять велику кількість умовних операторів (*if*), які тестують біти ітераційних ключів. Якщо частини цього оператора *then* та *else* виконуються за різний час, то, сповільнивши системний годинник і вимірявши тривалість усіх кроків, можна обчислити ключі ітерації. За цими ключами досить легко знаходиться загальний ключ. Незважаючи на те, що аналізи енергозатрат і часу виконання операцій можуть здатися дещо екзотичними, насправді виступають в ролі потужних методів, здатних зламати будь-який шифр, якщо він не має спеціального захисту.

Проведення криптоаналізу до давно відомих та нових криптоалгоритмів є актуальною задачею, оскільки своєчасне визначення криптостійкості досліджуваного алгоритму дозволить при потребі вдосконалити його або замінити на інший. Для виявлення нестійких криптоалгоритмів необхідно постійно вдосконалювати уже відомі методи криптоаналізу та знаходити нові.