УДК 003.26
Я. Литвиненко
(Тернопільський національний технічний університет імені Івана Пулюя)

АНАЛІЗ КРИПТОГРАФІЧНИХ МЕТОДІВ

Питання захисту інформації часто виникає під час створення та проектування інформаційних систем. З розвитком та поширенням глобальної комп'ютерної мережі Internet актуальним є питання захисту конфіденційної інформації користувачів комп'ютерних мереж. Тому, застосування програмних та апаратних засобів захисту інформації, що ґрунтуються на криптографічних методах є важливою та актуальною задачею.

Дана доповідь присвячена огляду та порівняльному аналізу методів шифрування інформації.

На даний час існує багато розроблених алгоритмів шифрування інформації. Зокрема, широко поширені такі:

- симетричні: DES, AES, ГОСТ 28147-89, Twofish, Blowfish, Camellia, IDEA, RC4 та інші;
- асиметричні: RSA, Elgamal;
- хєш-функції: MD4, MD5, MD6, SHA-1, SHA-2, ГОСТ Р 34.11-94.

Для їх порівняльного аналізу будемо використовувати наступні критерії:

- послідовний перебір можливих ключів дешифрування з метою відтворення вихідного тексту потребує значного часу обчислень або великих затрат на реалізацію цих обчислень;
- інформація про алгоритм шифрування не повинна впливати на стійкість до зламування системи шифрування;
- незначна зміна вихідного тексту повинна приводити до суттєвих змін шифрограми в разі використання одного і того ж ключа;
- структурні елементи алгоритму шифрування повинні бути незмінними;
- додаткові біти, які вводять у повідомлення в процесі шифрування, повинні бути надійно закриті в зашифрованому тексті;
- довжина зашифрованого повідомлення не повинна бути більшою, ніж саме повідомлення;
- не повинно бути простих залежностей між ключами, які послідовно використовують під час шифрування;
- довільний ключ із множини використовуваних ключів повинен забезпечувати надійність системи шифрування;

В наш час широко використовується методи шифрування інформації за допомогою симетричних і асиметричних криптосистем.

У багатьох країнах прийняті національні стандарти шифрування. Так, наприклад, в США використовується стандарт симетричного шифрування AES на основі алгоритма Rijndael з довжиною ключа 128, 192 і 256 біт. В Російскій Федерації діє прийнятий стандарт ГОСТ 28147-89, який використовує алгоритм блочного шифрування з довжиною ключа 256 біт, а також алгоритм цифрового підпису ГОСТ Р 34.10-2001.

Розглянувши основні види криптографічних методів згідно з запропонованими критеріями та проаналізувавши їх особливості, можна зробити висновок, що для більшості задач захисту інформації доцільно використовувати асиметричні методи шифрування даних, хоча симетричні методи мають ряд переваг і в певних випадках доцільніше використовувати саме ці методи шифрування.