УДК 004.056.55
Віктор Кубашок
Тернопільський національний технічний університет імені Івана Пулюя, Україна

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

Viktor Kubashok

CRYPTOGRAPHY PROTECTION OF INFORMATION SYSTEMS

Проблема захисту інформаційних ресурів в даний час набуває все більшого значення, необхідність використання криптографічних систем на підприємствах і в фінансових установах збільшується з кожним днем. Використання криптографічних методів захисту інформації дозволяє захистити програмну систему (ПС), або інший інформаційний ресурс від несанкціонованого доступу.

Криптографічний захист можна здійснювати різними способами: апаратним, програмним і апаратно-програмним.

Криптографічні алгоритми можна розділити на наступні категорії:

- алгоритми шифрування з секретним ключем (симетричні), які в свою чергу поділяються на блочні і поточні шифри;
- алгоритми шифрування з відкритим ключем (ассиметричні).

В основі більшості ітераційних блочних шифрів покладена ідея в побудові криптографічно-стійких систем шляхом застосування відносно простих криптографічних перетворень.

Основна ідея поточного шифрування є в тому, що над кожним із послідовності символів відкритого тексту здійснюється пертворення. В ідеалі над різнимим символами відкритого тексту здійснюються різноманітні перетворення, із кожним наступним моментом часу повинні змінюватися символи відкритого тексту. Реалізація здійснюється наступним чином, певний ключовий потік (keystream) або біжучий ключ (running key, RK) містить послідовність знаків $k_1,k_2,\ldots$, потім над кожним знаком x_1, відкритого тексту здійснюється перетворення, яке при потребі можна перетворити у вихідний текст, дане перетворення залежить від k_1 відповідноого знаку ключового потоку.

В асиметричній криптографіїї для зашифрування і розшифрування використовуються різні функції. Асиметричні алгоритми засновані на ряді математичних моделей, які в свою чергу надають їх стійкість, поки не буде знайдено поліноміальний алгоритм дані алгоритми будуть стійкі. Це ще визначає ще одну відмінність семетричного від асиметричного шифрування.

Щоб реалізувати багатофункціональну і багатокористувацьку інформаційну систему (ІС), при потребі необхідно буде отримувати від користувача інформацію, опрацьовувати її та виконувати необхідні дії, у такому випадку застосування криптографічних засобів є необхідним і при використанні даних механізмів інформаційна система буде стійкою.

Серед всього спектру способів захисту даних особливе місце займають криптографічні методи, їхня реалізаціє дозволяє відповідно до потреб зреалізувати необхідний функціонал для захисту персональної інформації. При реалізації інформаційної системи потрібно задати який алгоритм буде реалізований, як він буде взаємодіяти із програмною системою, як система буде взаємодіяти і користувачами. Криптографічні засоби дозволяють забезпечити захист ІС, дані механізми унеможливлюють несанкціонований доступ до персональних даних.