Удосконалення функції хешування MD4

УДК 004.056.2
Наталія Остапенко, Володимир Щербина

Національний авіаційний університет, natali.ost5@gmail.com

У наш час інформаційні технології займають важливе місце у нашому житті. Головними характеристиками інформації є конфіденційність, доступність та цілісність. Для контролю цілісності файлів операційних систем, програм чи даних широко використовуються функції хешування. Дані функції здійснюють стискання даних змінної довжини в послідовність фіксованого розміру (хеш-значення). Отримані хеш-значення використовується для перевірки відсутності модифікації даних. Незважаючи на велику кількість алгоритмів хешування, питання забезпечення криптографічної стійкості та високої швидкодії алгоритмів залишається відкритим. Тому розробка нових та удосконалення існуючих функцій хешування є актуальною задачею.

Метою даної роботи є підвищення ефективності захисту за рахунок удосконалення функції хешування MD4.

Для використання в криптографічних застосунках функція хешування повинна відповідати таким вимогам: 1) незворотність − для заданого значення функції хешування m має бути практично неможливо знайти повідомлення X, для якого $h(X) = m$; 2) стійкість до колізій першого роду – для одного хеш-значення, має бути практично неможливо підібрати для заданого повідомлення M друге повідомлення N, у яких є $h(N) = h(M)$; 3) стійкість до колізій другого роду − має бути практично неможливо підібрати пару повідомлень (M, M'), для яких хеш-значення будуть однакові $h(M) = h(M')$.

Однією з відомих функцій хешування є MD4, розроблена Рональдом Рівестом в 1990 році, і вперше описана в RFC 1186. Цей алгоритм використовувався в протоколі аутентифікації MS-CHAP, розробленому корпорацією Майкрософт для виконання процедур перевірки автентичності віддалених робочих станцій Windows. MD4 створювався передусім як дуже швидкий алгоритм хешування, але він не задовольняє вимог до криптографічних функцій хешування та може піддаватися криптоаналізу.

У роботі запропоновано алгоритм хешування, який розроблено на основі MD4. Даний алгоритм частково зберіг основну структуру, але отримав декілька нововведень: 1) при стисненні замість чотирьох 32-бітних змінних A, B, C, D запропоновано використання п'яти 64-бітних змінних A, B, C, D, J; 2) збільшено довжину хеш-значення до 256-біт; 3) збільшено кількість етапів виконання стиснення; 4) замінені додаткові функції F, G, H; 5) додані додаткові операції на кожному етапі.

Таким чином, запропоновано нову функцію хешування, що дозволить підвищити ефективність захисту інформації. Далі плануються дослідження для перевірки стійкості та швидкодії даної функції хешування.