УДК 681.3.06:519.248.681

І. Д. ГОРБЕНКО, д-р техн. наук, О. А. ЗАМУЛА, канд. техн. наук,
Є. В. ПОПОВИЧ, Т. О. ГРІНЕНКО

МЕТОДИ ЗАБЕЗПЕЧЕННЯ АВТЕНИЧНОСТІ З ВВЕДЕННЯМ НАДЛИШКОВОСТІ

Згідно з основними положеннями міжнародних та державних стандартів системи захисту інформації повинні надавати користувачам такі послуги, як цілісність, доступність та спостережність. Одним із основних методів забезпечення цих послуг є застосування процедур та алгоритмів автентифікації. На сьогодні теорія та практика автентифікації одержали значний розвиток [1-3]. Але досі немає робіт, в яких методи автентифікації розглядались би в порівнянні. Метою даної статті є класифікація, характеристика та порівняння відомих методів автентифікації інформації, яка обробляється та передається з введенням надлишковості.

Аналіз низки джерел показав, що автентифікація повідомлення M_i на основі надлишковості може бути забезпечена за рахунок використання:

- однонаправленої хешфункції (h);
- ключових хешфункцій або кодів автентифікації ($КА$);
- цифрового підпису ($ЦП$);
- іншої надлишкової інформації, що формується відповідно з прийнятими правилами, які будемо називати контрольною сумою ($КС$).

Позначимо автентифіковане повідомлення, як M_i^A та розглянемо суть та відмінні риси методів та реалізованих на їх базі алгоритмів.

1. Автентифікація з використанням однонаправлених хешфункцій

Як відомо під однонаправленою хешфункцією розуміється відображення інформації M_i в її стислий образ h:

$$h=H(M_i), \tag{1}$$

де H – функція стиснення (розтиснення) M_i в h.

Особливістю такого відображення є те, що прямий розрахунок, відповідно до (1), повинен носити не більш, ніж поліноміальну складність. У випадку, коли довжина повідомлення менша за довжину хешфункції ($l_m<l_h$), функція H – розтискаюча, а коли довжина повідомлення більша за довжину хешфункції ($l_m>l_h$), функція H – стискаюча.

Довжина l_h, як правило, фіксована, або має декілька фіксованих значень (128, 160, 256 біт) та не залежить від довжини повідомлення.

Однонаправлена функція повинна бути стійкою проти криптоаналітичних атак, основними з яких є:

1. Стійкість проти знаходження прообразу повідомлення M_i:

$$M_i=H^{-1}(h), \tag{2}$$

при відомому значенні хеш-функції.

Складність таких розрахунків повинна бути не нижче за субекспоненціальну складність.

2. Стійкість за другим прообразом, яка заключається в тому, що при відомій $h=H(M_i)$ необхідно знайти таке повідомлення M_j, для якого

$$H(M_i)=H(M_j). \tag{3}$$

Задача пошуку такого повідомлення повинна носити не нижчу за субекспоненціальну складність.

3. Стійкість до колізій, суть якої заключається в складності знаходження двох повідомлень M_i та M_j, для яких

$$H(M_i)=H(M_j). \tag{4}$$

Задача пошуку таких повідомлень повинна бути експоненціально складною.

З вищезазначеного можна зробити такі висновки:

1. Застосування автентифікації на основі однонаправленої хеш-функції дозволяє забезпечити аутентичність (цілісність та достовірність) на підставі внесення та додавання до повідомлення M_i інформації h .

2. Автентифіковане повідомлення M_i^A є сукупність інформацій M_i та h ($M_i^A=\{M_i, h\}$).

3. При використанні однонаправленої хешфункції здійснюється відображення "багато в одне", тобто в конкретне значення хешфункції h може відобразитись велика кількість повідомлень.

4. Відповідно до парадоксу дня народження [1] для однонаправленої хешфункції існує атака типу колізій, розрахункова складність якої для повідомлення з основою алфавіту m має вигляд:

$$I \cong \sqrt{m^{l_h}}, \tag{5}$$

та з основою $m=2$:

$$I \cong \sqrt{2^{l_h}}. \tag{6}$$

Проведений аналіз показує, що розв'язання задач автентифікації та шифрування, наприклад, в безумовно стійкій системі, у випадку використання однонаправленої хешфункції, повинен складатись з наступних кроків:

1. Для повідомлення M_i розраховується хешфункція h та формується автентифіковане повідомлення M_i^A.
2. Далі повідомлення M_i^A зашифровується, наприклад, в системі Вернама [3].
3. При отриманні повідомлення розшифровується в системі Вернама.
4. Для розшифрованого повідомлення $M_i^{A'}=\{M_i', h\}$ розраховується хешфункція $h'=H(M_i')$.
5. Здійснюється порівняння розрахованої хешфункції h' та h, яка знаходиться при повідомленнях. В разі збігання даних хешфункцій повідомлення вважається достовірним та цілісним, в протилежному випадку повідомлення таким не вважається.

На цей час розроблена велика кількість однонаправлених хешфункцій основними з яких є: MD4, MD5, RIPEMD-128, SHA-1, RIPEMD-160, ГОСТ 34.311-95 [1-3].

Як показує аналіз даних хешфункцій, всі вони є середньоскладними, мають поліноміальну складність та забезпечують допустимі швидкості хешірування. Оцінка стійкості, в сенсі захищеності від обману під час знаходження колізій (6) за використанням оцінки Сіменсона [3], є:

$$P_{обм} \geq 2^{-l_h}. \tag{7}$$

Таблиця 1

Назва хешфункції	Довжина (біт)	Ймовірність обману
MD4	128 (256)	$3\cdot10^{-39}$
MD5	128	$3\cdot10^{-39}$
RIPEMD-128	128	$3\cdot10^{-39}$
SHA-1	160	$6{,}8\cdot10^{-49}$
RIPEMD-160	160	$6{,}8\cdot10^{-49}$
ГОСТ 34.311-95	256	$3\cdot10^{-77}$

В табл. 1 наведені значення ймовірності обману, які розраховані відповідно до (5) та (6) для вказаних хеш-функцій.

Даний метод є симетричним, оскільки не забезпечує реалізацію моделі взаємної недовіри. Він може використовуватися в разі, коли користувачі системи довіряють один одному.

2 Автентифікація з використанням ключових хешфункцій

У випадку, коли для забезпечення автентифікації надлишковість вноситься за рахунок використання ключових хешфункцій або кодів автентифікації (КА) [2], виникають деякі розходження з розглянутими раніше однонаправленими хешфункціями. Основною різницею є то, що:

$$KA=H(M_i, K_j). \tag{8}$$

Для ключової хешфункції основною перевагою є захищеність від атаки типу колізій. Для оцінки якості забезпечення автентифікації можна користуватися співвідношенням (8), але крім довжини хешфункції l_h, необхідно враховувати довжину ключа автентифікації l_{KA} та вибрати з них той показник, який приводить до найбільшої ймовірності обману. Оскільки для ключової хешфункції відсутня атака типу колізій, то довжина l_{KA} може бути менша за l_h при забезпечені тієї ж стійкості.

Ключова хешфункція є симетричною. Тому, відповідно, ключ автентифікації у всіх абонентів повинен бути однаковим і, як наслідок, за допомогою цієї функції не можливо забезпечити модель взаємної недовіри.

В якості ключових хешфункцій можна назвати наступні: MDC-2, MDC-4, DES в режимі роботи коду автентифікації, ГОСТ 28147 в режимі виробки імітовставки.

В табл. 2 наведені значення ймовірності обману для ключових хешфункцій, отриманих відповідно до співвідношення (7).

Таблиця 2

Назва алгоритму	Довжина ключа (біт)	Довжина імітовставки (біт)	Ймовірність обману
MDC-2	56	128	$1{,}4\cdot10^{-17}$
MDC-4	56	128	$1{,}4\cdot10^{-17}$
DES	56	64	$5{,}4\cdot10^{-20}$
ГОСТ 28147	256	64	$5{,}4\cdot10^{-20}$

Безпосередньо реалізація системи захисту з забезпеченням автентифікації на основі ключової хешфункції виконується аналогічно, як і для однонаправленої хешфункції. Різниця лише в тім, що отримувач повинен володіти ключем автентифікації *Kj*. В алгоритмах ГОСТ 28147, RIENDAEL, IDEA, DES, передбачено стандартний режим створення (виробітка) ключової хешфункції.

3. Автентифікація з використанням цифрового підпису

Суть цього метода автентифікації полягає в обчисленні для кожного повідомлення або інформації цифрового підпису [1]. Відмінною рисою цього методу є те, що цифровий підпис являє собою криптоперетворення від хешфункції *h*, особистого ключа $K_л$ та інших параметрів *Pr*:

$$ЦП=F(H(M),K_л,Pr,. \qquad (9)$$

де *H(M)* – як правило однонаправлена хешфункція; $K_л$ – особистий ключ відправника або автора повідомлення; *Pr* – додаткові параметри, в якості яких можуть використовуватися ідентифікатори відправника та одержувача, час створення та відправки повідомлення, час життя повідомлення, символи керування і т.і.

При використанні цифрового підпису може бути реалізована модель взаємної недовіри, взаємного захисту завдяки тому, що кожен користувач може генерувати сам собі необхідну пару ключів (особистий – секретний та загальний – відкритий). Особистий ключ зберігається в таємниці та не випускається з під контролю. Відкритий ключ розсилається безпосередньо або через відповідний центр у вигляді сертифікатів всім іншим користувачам.

Створити повідомлення може лише користувач, що володіє особистим ключем, перевірити цілісність та достовірність (автентифікувати) повідомлення може кожен, хто володіє відкритим ключем.

Аналіз показує, що, з точки зору складності розрахунків, цифровий підпис у порівнянні з розрахунками однонаправленої або ключової хешфункції має складність на декілька порядків більшу, а здійснення цифрового підпису вимагає більш потужних ресурсів, а також багатослівної арифметики.

При цьому, попередній аналіз показує, що:

1. Використання цифрового підпису в системах захисту забезпечує найбільшу стійкість автентифікації. Це пов'язано з тим, що цифровий підпис шифрується разом з повідомленням, і виділити його без знання ключа практично не можливо. В цьому випадку відсутні аналітичні атаки, крім атаки типу брутальна сила.

2. У випадку реалізації моделі взаємної недовіри та взаємного захисту складність криптоаналітичної атаки, метою якої є підробка цифрового підпису, зводиться до задачі, що стала вже класичною, субекспоненціального та експоненціального. Зокрема, при використанні цифрового підпису на базі RSA алгоритму та застосуванні методу загального решета числового поля [2], складність факторизації можна визначити формулою:

$$I=exp(\delta(\ln N)^{\nu}(\ln\ln N)^{1-\nu}), \qquad (10)$$

де *N* – модуль перетворення; ν – параметр, що залежить від методу вирішення задачі; δ – константа (залежить від використаного математичного методу).

При використанні протоколу Діфі-Хелмана основна частина процесу криптоаналізу складається з вирішення дискретно-логарифмічного порівняння виду

$$Y=(a^X) \bmod p, \qquad (11)$$

де *Y* – відкритий ключ; *a* та *p* – загальномережеві параметри; X – особистий ключ.

Задача криптоаналізу складається з находження особистого ключа

$$X=(\log_a Y) \bmod p. \qquad (12)$$

Складність вирішення такої задачі залежить від математичного апарату, який використовується, а також від потужності обчислювальної системи та програмної платформи.

Достатньо прийнятою апроксимацією складності є співвідношення (10) з відповідно вибраними параметрами δ та ν.

Очевидно, що найбільш перспективним є цифровий підпис, який реалізований в класі перетворень еліптичних кривих над розгорнутим полем [2]. У цьому випадку основною відзнакою від вищезазначених алгоритмів є те, що розмір модуля перетворень може бути значно зменшений до розмірів $\approx 2^{163}/2^{257}$ [2]. Крім того, до таких же розмірів може бути зменшена довжина загального та особистого ключів. Основною перевагою цифрового підпису на базі еліптичних кривих є те, що складність криптоаналізу для нього залишається експоненціальною та оцінюється для оптимального методу Поларда [2], як:

$$I=\sqrt{\frac{\pi n}{4}}, \qquad (13)$$

де n – порядок базової точки.

В нашому випадку n може приймати значення 2^{160}-2^{256}.

4. Автентифікація з використанням контрольних сум

Особливістю даного методу автентифікації є те, що для повідомлення розраховуються некриптографічні контрольні суми невеликого обсягу. Аналіз джерел [1-3] показує, що їх можна віднести до однонаправлених хешфункцій, оскільки контрольна сума розраховується аналогічно до співвідношення (1). Але такі контрольні суми не є розрахунково та колізійно стійкими, тобто для них може бути вирішена задача типу (2), завдяки чому в криптосистемах вони мають досить обмежене використання.

Висновок

Таким чином, проведений аналіз показав, що задача автентифікації є самостійною криптографічною задачею та потребує окремого розгляду.

На цей час немає єдиної теорії автетифікації, тобто забезпечення цілісності та достовірності інформації на всіх її життєвих етапах. В якості оцінки можуть використовуватися оцінки, які надає теорія Сімонсона.

Проведений аналіз показав, що існує декілька методів забезпечення автентичності повідомлень. В якості основної ознаки їх класифікації можна використати застосування або незастосування надлишковості. Проведений вище аналіз показав, що надійна автентифікація може бути забезпечена лишу під час застосування надлишковості.

За способом формування надлишковості методи можна поділити на однонаправлені та ключові. Відмінною ознакою є те, що ключові хешфункції потребують використання симетричних криптоперетворень та ключа.

Для моделі взаємної недовіри та взаємного захисту може використовуватися лише цифровий підпис.

Використання будь якого методу автентифікації необхідно узгоджувати з моделлю загроз, політикою інформаційної безпеки та політикою надання послуг користувачам.

Список література: 1. *Brown L.*, LOKI – a cryptographic primitive for authentication and secrecy application in Proceedings of AUSCRYPT 90, 1990. 2. *Krawczyk H.*IETF Draft: Keyed-MD-5 for Message Autentification, November, 1995. 3. *Симонс Г. ДЖ.* Обзор методов аутентификации // ТИИЭР. 1988. №5. С.105-125.

Харківський державний технічний університет радіоелектроніки

Надійшла до редколегії 5.04.2001