УДК 004.056.53

ВИКОРИСТАННЯ КРИПТОГРАФІЧНОГО МЕТОДУ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Коленко В.В.
Одеський національний політехнічний університет

В статті визначено проблеми достовірності інформації в електронному документообігу та розглянуто підхід до розробки криптографічного алгоритму на основі технології хешування. Наведено основні вимоги щодо властивостей криптографічного алгоритму Представлено узагальнену схему роботи алгоритму хешування та запропоновано метод захисту електронних документів на основі хешування та використання MD5.
Ключові слова: *криптографія, хешування, захист інформації.*

Постановка проблеми в загальному вигляді і її зв'язок з важливими науковими або практичними завданнями. Система документообігу сучасного підприємства або організації має електронний вигляд і містить сканкопії документів на паперових носіях та електронні документи, які надходять до організації або створюються в результаті функціонування. Оскільки захисту потребують всі види документів, то необхідно розглядати проблему цілісності інформації та основні види атак на системи документообігу і засобів протидії.

На сьогоднішній час можна виділити дві основні задачі захисту цілісності інформації та підтвердження авторства цифрових даних.

Перша відноситься до інформаційного обміну в умовах взаємної довіри сторін. У цьому випадку необхідно забезпечити механізм, який дозволяє отримувачу бути впевненим, що дані прийшли від відправника та не є достовірними. Друга – в отримувача не повинно бути можливості створення недостовірних даних від імені відправника. Така постанова задачі передбачає відсутність довіри між сторонами.

Підходи та методи рішення обох видів задач істотно розрізняються. Наслідком даної ситуації стає об'єктивна потреба в дослідженні, перегляді й переосмисленні існуючих підходів, методологій і технологій розробки, впровадження методів захисту інформації. Важливим завданням даної роботи стає вдосконалення методу рішення проблеми захисту авторських прав за допомогою електронного цифрового підпису.

Аналіз останніх досліджень і публікацій і виділення невирішених завдань проблеми. Існуючі системи криптографічних стандартів передбачають алгоритми імітозахисту – захисту від нав'язування противником помилкових даних. Ця ж методика дозволяє підтвердити авторство інформації в умовах взаємної довіри між відправником та отримувачем, але не захищає її від підробки з боку отримувача. Саме тому її іноді називають «симетричним цифровим підписом». Тому для вирішення проблеми захисту інформації можна застосувати метод впровадження та перевірки електронного цифрового підпису (ЕЦП). В схемах ЕЦП замість документа розглядається його хеш-функція h(x), основна властивість якої – практична неможливість створення двох різних документів з однаковим значенням. Перевірка оригінальності документа полягає у контролі співвідношення, який за допомогою спеціального програмного забезпечення підтверджує достовірність інформації документа, його реквізитів і факту підписання конкретною особою [1].

Формулювання цілей статті. Мета інформаційної безпеки – забезпечити цілість системи електронного документообігу, захистити і гарантувати точність та повноту інформації, мінімізувати можливі руйнування, якщо інформація буде модифікована або пошкоджена. Інформаційна безпека вимагає обліку всіх подій, в ході яких інформація створюється, модифікується, до неї забезпечується доступ або вона поширюється. Проблема збереження електронних документів від копіювання, модифікації і підробки вимагає для свого вирішення специфічних засобів і методів захисту [2].

Виклад матеріалів дослідження. Найбільш поширеними та ефективними є криптографічні методи захисту інформації. Процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється істотно більшою вартістю, проте її властивостями і перевагами є висока продуктивність, простота, захищеність, але програмна реалізація більш практична. Для сучасних криптографічних систем захисту інформації сформульовані наступні загальноприйняті вимоги:

– зашифроване повідомлення повинне піддаватися читанню лише за наявності ключа;

– число операцій, необхідних для визначення використаного ключа шифрування по фрагменту шифрованого повідомлення і відповідного йому відкритому тексту, має бути не менше загального числа можливих ключів;

– число операцій, необхідних для розшифровки інформації шляхом перебору ключів повинно мати строгу нижню оцінку і не виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості мережевих обчислень);

– знання алгоритму шифрування не повинне впливати на надійність захисту;

– незначна зміна ключа повинна приводити до істотної зміни вигляду зашифрованого повідомлення навіть при використанні одного і того ж ключа;

– структурні елементи алгоритму шифрування мають бути незмінними;

– додаткові біти, що вводяться в повідомлення у процесі шифрування, мають бути повністю і надійно приховані в шифрованому тексті;

– довжина шифрованого тексту має бути рівною довжині вихідного тексту;

У схемах симетричної криптографії, зокрема в алгоритмах шифрування і створення імітовставки, обидва учасники інформаційного обміну поділяють єдиний секретний ключ, який можна створювати як простий масив з випадкових або псевдовипадкових бітів. Асиметрія ролей відправника і отримувача в схемах ЕЦП вимагає наявності двох тісно пов'язаних ключів: секретного або ключа підпису і відкритого, або ключа перевірки підпису. Другий з них ключем не є, оскільки ключ за визначенням зобов'язаний бути секретним. Будь-яка схема ЕЦП повинна визначити три наступних алгоритми:

– алгоритм генерації ключової пари для підпису та її перевірки;

– алгоритм підпису;

– алгоритм перевірки підпису.

Останні досягнення теорії обчислювальної складності показали, що загальна проблема логарифмування в дискретних полях, що є базою ЕЦП, не може вважатися досить міцною. Наприклад, розміри блоків, що вважаються «безпечними», зростають порівняно швидкими темпами. В результаті це призвело до того, що стандарти ЕЦП переведені на еліптичні криві [3]. Схеми ЕЦП при цьому залишилися колишніми, але в якості чисел, якими вони оперують, тепер використовуються не елементи кінцевого поля, а еліптичні числа – рішення рівняння еліптичних кривих над зазначеними кінцевими полями. Роль операції піднесення числа в ступінь в кінцевому полі в оновлених стандартах виконує операція взяття кратної точки еліптичної кривої – «множення» точки на ціле число [4].

Належний вибір типу еліптичної кривої дозволяє багаторазово ускладнити завдання викриття схеми ЕЦП і зменшити робочий розмір блоків даних, що призводить до більшої стійкості. Блоки даних, які можуть бути підписані безпосередньо, обмежені за розміром: вони не можуть виходити за межі використовуваної при роботі алгоритмів розрядної сітки. У той же час може виникнути потреба розробки ЕЦП для документа довільного розміру. Щоб подолати це обмеження, в схемах ЕЦП прийнято підписувати не безпосередньо електронний документ, а результат його перетворення до блока даних фіксованого розміру, званого хешем (hash) повідомлення. Функція виду $y=f(x)$ називається криптографічною хеш-функцією, якщо вона задовольняє наступним властивостям:

– на вхід хеш-функції може поступати послідовність даних довільної довжини, результат же (званий *хеш*, або *дайджест*) має фіксовану довжину;

– значення *y* по наявному значенню *x* обчислюється протягом поліноміального часу, а значення *x* за наявним значенням *y* майже у всіх випадках обчислити неможливо;

– розрахунково неможливо знайти два вхідні значення хеш-функції, що дають ідентичні хеші;

– під час обчислення хеша використовується вся інформація вхідної послідовності;

– опис функції є відкритим і загальнодоступним.

Алгоритм хешування повинен мати такі властивості, як:

– постійність розміру – для вхідного масиву даних довільного розміру результатом має бути блок даних фіксованого розміру;

– обчислювальна необоротність – для заданого хеша не повинно бути способу підбору масиву даних під нього більш ефективним способом, ніж перебір по можливим значенням масиву даних;

– свобода від колізій – не повинно існувати обчислювально ефективного способу пошуку двох масивів даних з однаковим значенням хеша [4].

У ході дослідження для загального алгоритму шифрування, було обрано технологію MD5. Основний принцип розробленого алгоритму полягає в тому, що на вхід алгоритму надходить вхідний потік даних, хеш якого необхідно знайти. Довжина повідомлення може бути будь-якою (у тому числі нульовою). Запишемо довжину повідомлення в L. Це число ціле і невід'ємне. Кратність необов'язкова. Після надходження даних йде процес підготовки потоку до обчислень.

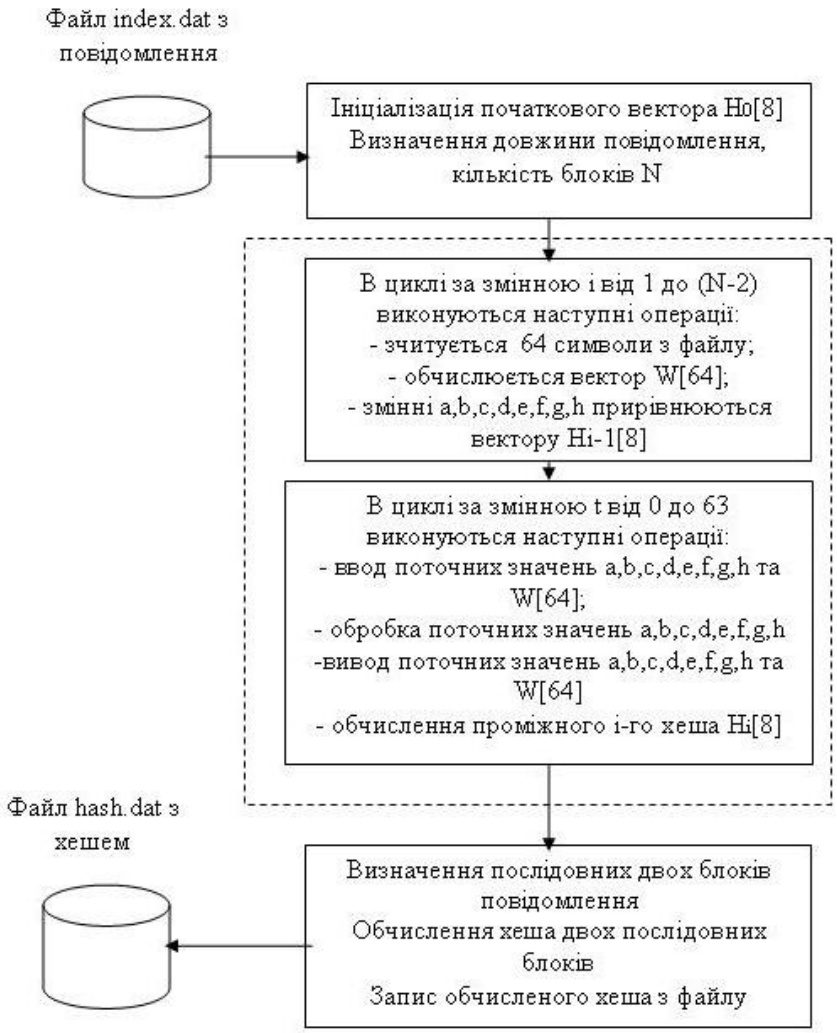

Рис. 1 – Узагальнена схема роботи алгоритму хешування

Основні етапи алгоритму хешування (рис. 1): ініціалізація початкового вектора; визначення довжини повідомлення; обчислення вектора; обчислення проміжного хешу; визначення послідовних блоків; обчислення послідовних блоків; запис обчисленого хешу з файлу.

У ході дослідження було розроблено метод захисту електронних документів на основі хешування та використання MD5 (рис. 2). Криптографічна хеш-функція використовується тут як засіб контрольного підсумовування: наприклад, для деякого файлу, розміщеного в публічний доступ на ftp-сервері, може бути подано його хеш, вирахуваний з використанням деякого алгоритму. У такому випадку користувач, що завантажив даний файл, може переконатися в його автентичності. Проте зловмисник може підмінити файл і опублікувати хеш, що відповідатиме новому файлу – виявити подібні маніпуляції, використовуючи звичайні хеш-функції, неможливо. Захист від подібного роду атак забезпечується шляхом застосування кодів перевірки автентичності.

Кодами перевірки автентичності, або MAC-кодами, є криптографічні хеш-функції, для обчислення яких необхідно знати секретний ключ. Використання ключа дозволяє гарантувати неможливість підміни об’єктів, що захищаються, як було описано вище: зловмисник, що не знає секретного ключа, не зможе перерахувати хеш для нового файлу. У якості кодів перевірки автентичності часто використовуються модифікації симетричних криптографічних систем.

Рис. 2 – Метод захисту електроних документів

Висновки та перспективи використання. Захист інформації в системах електронного документообігу – нагальна потреба функціонування сучасного підприємства або організації. Вибір конкретних засобів захисту залежить від цінності інформації, яка оберігається. Тому при виборі методів та засобів захисту слід оцінити реальні втрати від розголошення або спотворення інформації.

В процесі роботи над загальним алгоритмом шифрування було виконано всі умови, які відносяться для такого ряду завдань. Але отриманий алгоритм має експериментальний характер, та з часом може пройти деякі етапи технічного удосконалення, оскільки використання MD5 має на увазі вирішення проблеми можливих колізій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Брюс Шнайдер. Прикладная криптография. [Текст] – М. : Диа Софт, 2000. – 368 с.

2. Коленко, В. В. Математические модели и методы процессов защиты информации [Текст] / В. В. Коленко, О. В.Нарожний, Г. Ф.Сафонова // Збірник наукових праць / Інформаційні технології в освіті, науці та виробництві – Вип. 1 – Одеса, 2012 .

3. Ярочкин В. И. Информационная безопасность [Текст] / В. И. Ярочкин. – М. : Междунар. отношения, 2000. – 4000 с.

4. Домарев В. В. Безпека інформаційних технологій. Системний підхід [Текст] / В. В. Домарев. – К. : ТОВ «ТВД», 2004. – 992 с.

Коленко В.В., ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКОГО МЕТОДА ЗАЩИТЫ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

В статье определены проблемы достоверности информации в электронном документообороте и рассмотрен подход к разработке криптографического алгоритма на основе технологии хеширования. Приведены основные требования относительно свойств криптографического алгоритма. Представлены обобщенную схему работы алгоритма хеширования и предложен метод защиты электронных документов на основе хеширования и использования MD5.

Ключевые слова: *криптография, хеширования, защита информации*

Kolenko V.V. APPLICATION IN THE CRYPTOGRAPHIC ALGORITHM WORK FOR DATE FILES

In the article the problems of information reliability in an electronic document and the approach to the design of cryptographic algorithm technology based hashing are defined. There are given major requirements for the properties of the cryptographic algorithm. The generalized scheme of the hashing algorithm and the method of electronic documents protection based on hashing and use of MD5 is presented.

Keywords: *cryptography, hashing, data protection.*

Статтю прийнято
до редакції 27.06.14