УДК 004.62

Л.А. Шувалова, С.Ю. Куницька, І.І. Білас

Черкаський державний технологічний університет, Черкаси

ВИБІР МЕТОДУ ШИФРУВАННЯ ДЛЯ ЗАДАЧІ ОПТИМІЗАЦІЇ СИСТЕМИ ОБ'ЄКТИВНОГО КОНТРОЛЮ ТЕХНОЛОГІЧНОГО ПРОЦЕСУ

Проведено дослідження симетричні алгоритми шифрування інформації та асиметричні алгоритми шифрування інформації На основі проведеного дослідження обрано алгоритм шифрування інформації для задачі оптимізації системи об'єктивного контролю технологічного процесу. Проведено дослідження використання хешування в програмі оптимізації системи контролю технологічного процесу та вибір оптимального методу для даної задачі Для забезпечення імітозахисту для даної задачі обрано використання хешування MB5.

Ключові слова: *шифрування, алгоритм шифрування, криптографічна система, хешування.*

Вступ

Постановка завдання. Для забезпечення об'єктивності контролю технологічного процесу переробки продукції, можливості технічної обробки його результатів, оперативності і точності оцінок, використання показника якості в економічних розрахунках необхідно подати їх у вигляді масиву цифрових даних, що можуть відображати як абсолютну величину окремих показників, так і деякі відносні показники. Такі завдання можуть бути вирішені на базі квалімегричної оцінки якості. У результаті ряду впорядкованих операцій з вибору, вимірюванню та оцінці властивостей досліджуваного об'єкта кваліметрія дає можливість отримати показник його якості у вигляді деякої цифрової величини, що дозволяє використовувати її в алгоритмі управління технологічним процесом. Автоматизація процесів харчових технологій призвела до створення пристроїв, що дозволяють реєструвати накопичення, розпад і взаємодію різних речовин та зміну їх стану при найнижчих концентраціях.

Для постійного контролю та необхідності зберігання отриманих масивів цифрових даних виникає питання зменшення їх обсягу для ефективного зберігання на цифрових носіях, а також забезпечення конфіденційності отриманої інформації. Для вирішення цих питань використовують скорочення надмірності інформації, що є основою її стиснення, та шифрування даних, що перетворює дані, з метою приховання інформації. .Алгоритми шифрування завдяки обробці певним чином відкритої інформації практично унеможливлюють несанкціонований доступ до неї без спеціального ключа [1].

Для забезпечення належного рівня безпеки даних показників якості технологічного процесу ключ шифрування є доступним лише обмеженим колам осіб і змінюється через певний період часу.

Результати досліджень

1. Дослідження методів шифрування. 1.1. Симетричні алгоритми шифрування інформації.

Шифрування з симетричними ключами - схема шифрування, у якій ключ шифрування, та ключ дешифрування збігаються, або один легко обчислюється з іншого та навпаки.

Симетричні алгоритми шифрування можна розділити на потокові та блочні алгоритми шифрування. Потокові алгоритми шифрування послідовно обробляють текст повідомлення. Блочні алгоритми працюють з блоками фіксованого розміру. ***Як*** правило, довжина блоку дорівнює 64 бітам, але, в алгоритмі AE8 (Асіуапсесі Епсгургіоп Зіапсіагсі) використовуються блоки довжиною 128 біт.

Сьогодні існує досить багато симетричних алгоритмів криптографічного захисту інформації, які широко використовуються в сучасних архіваторах. Серед них можна виділити Тгіріе OE8 (Вага Епсгургіоп Бгапсіагсі), ШЕА (Іпіетаїіопаї Вага Епсгургіоп А1§огігЬт), В1о\уїї$Ь, Сазі-128 і деякі з AE8, включаючи новий AE8 Купсіаеі поряд з 21Р-стисненням. А якщо говорити про методи шифрування, реалізовані в програм ах-архіваторах, то тут вибір більш обмежений. У переважній більшості випадків в популярних архіваторах реалізований якийсь один метод. Найчастіше це ЛР-шифрування або AE8 Кіркіаеі. Виняток становить Ро\уєгАгсЬіуєг, в якому користувачеві надається цілих 5 варіантів кодування стислих даних: Віолуйзь (128 біт), БЕЗ (64 біт), Тгіріе БЕ8 (128 біт) і Купсіаеі AE8 (128 біт) і звичайне ЛР-шифрування. Слід визнати, що стандартне 2ЇР-шифрування не відноситься сьогодні до числа надійних, так само як і шифрування із застосуванням алгоритму БЕ8. Починаючи з середини 90-х років, стали з'являтися кандидати на заміну ВЕ8, найбільш відомі з яких - Тгіріе БЕ8, ЮЕА і В1о\уйз1і. Перший і останній застосовуються і сьогодні в різних програмних засобах для шифрування даних, у тому числі в архіваторах. ЮЕА використовується РОР (РгеПу Ооосі Ргіуасу) і рядом інших криптографічних програм. Тгіріе ИЕ8 («потрійний БЕ8», бо тричі шифрує інформацію «звичайним» алгоритмом OE8) вільний від основного недоліку колишнього варіанта - короткого ключа. Тут ключ в 2 рази довше, і тому надійність «потрійного» OE8 набагато вище. Але

Тгіріе ОЕ8 успадкував і слабкі сторони свого попередника - відсутність можливостей для паралельних обчислень при шифруванні і низьку швидкість.

Сучасний 64-бітний блоковий шифр ВІо^йзЬ з ключем змінної довжини від 32 до 48 біт в наш час вважається досить сильним алгоритмом. Він був розроблений в 1993 році в якості заміни вже існуючих алгоритмів і є набагато більш швидким, ніж ИЕ8, Тгіріе ОЕ8 і ШЕА.

Однак найбільш надійним сьогодні визнається Яцпсіаеі - новий стандарт шифрування АЕ8. Він має 3 розміру ключа: 128, 192 і 256 біт і володіє масою переваг. До їх числа відносяться висока швидкість шифрування, мінімальні вимоги до обчислювальних ресурсів, стійкість до атак і легка розширюваність (при необхідності можна збільшити розмір блоку або ключа шифрування). Більше того, в найближчому майбутньому АЕ8 Купсіаеі залишиться самим надійним методом, оскільки якщо навіть припустити, що з'явиться комп'ютер, здатний перевірити 255 ключів в секунду, то буде потрібно приблизно 149 трильйонів років, щоб визначити 128-бітний ключ АЕ8 [2].

1.2. Асиметричні алгоритми шифрування інформації. *Асиметричні алгоритми шифрування* **- це** певний клас алгоритмів, що використовуються в системах криптографічного захисту даних, що мають таку особливість: для зашифровування даних використовується один ключ, а для розшифровування - інший ключ (звідси і назва - асиметричні). Перший ключ є відкритим і може бути опублікованим для використання користувачами системи, які шифрують дані. Тому системи криптографічного захисту, що використовують асиметричні алгоритми шифрування, називають ще криптосистемами з відкритим ключем. Розшифровування даних за допомогою відкритого ключа неможливе. Для розшифровування даних отримувач зашифрованої інформації використовує другий ключ, який є секретним. Ключ розшифровування не може бути визначеним з ключа зашифровування.

Головне досягнення асиметричного шифрування полягає в тому, що воно дозволяє людям, що не мають наперед наявної домовленості про безпеку, обмінюватися секретними повідомленнями. Необхідність відправникові й одержувачеві погоджувати таємний ключ по спеціальному захищеному каналі цілком відпадає. Прикладами криптосистем з відкритим ключем є Е1§ата1 (названа на честь автора, Тахіра Ельгамаля), К8А (названа на честь винахідників: Рона Рівеста, Аді Шаміра і Леонарда Адлма- на), ВіШе-НеІІтап і Б8А, Оі§іІа1 8і§даПіге АІ^огіІЇїт (винайдений Девідом Кравіцом).

Загалом алгоритми криптосистем з відкритим ключем можна використовувати як самостійний засіб для захисту переданої і збереженої інформації, як засіб розподілу ключів (зазвичай за допомогою алгоритмів криптосистем з відкритим ключем розподіляють ключі, малі за обсягом, а саму передачу великих інформаційних потоків здійснюють за допомогою інших алгоритмів) та для автентифікації користувачів.

Практичне використання асиметричних алгоритмів шифрування в архіваторах загального призначення обмежено повільністю цього класу алгоритмів у порівнянні з симетричними. Тому безпосереднє самостійне використання криптосистем з відкритим ключем є доцільним за наявності спеціальних визначених наперед вимог до створення таких систем та критеріїв, що забезпечує цей клас алгоритмів шифрування [3].

2. Алгоритм шифрування інформації для даної задачі. Криптосистема Я8А стала першою системою, придатною одночасно і для шифрування, і для організації цифрового підпису. Алгоритм використовується у великому числі криптографічних додатків, включаючи РОР, 8/МІМЕ (8есиге / Миїїіригрозе Іпїетеї Маіі Ехіепзіопв), ТЬ8/88Е (Тгапзрогї Ьауег 8есшїїу / 8оскеі5 Ьауег), 1Р8ЕС/ІКЕ (Іпіетеї Ргоіосої 8есигіїу / ітегпеї Кеу ЕхсЬап^е) та інших. Алгоритм К.8А ґрунтується на обчислювальній складності задачі факторизації добутку двох великих цілих чисел. Він заснований використанні так званих односторонніх функцій, які мають таку властивість:

1. Якщо відомо х, то Г(х) обчислити відносно просто.

2. Якщо відомо у = Г(х), то для обчислення Х немає простого (ефективного) шляху.

Під односторонністю розуміється не теоретична односпрямованість, а практична неможливість обчислити зворотне значення, використовуючи сучасні обчислювальні засоби, за доступний інтервал часу.

Для шифрування використовується операція зведення в ступінь по модулю великого числа. Щоб дешифрувати за розумний час (зворотної операції) необхідно вміти обчислювати функцію Ейлера від даного великого числа, для чого необхідно знати розкладання числа на прості множники.

У криптографічній системі з відкритим ключем на основі алгоритму Я8А використовується як *відкритий ключ (ривІіс кеу),* так і *закритий ключ (ртаіе кеу),* кожен з яких складається з пари цілих чисел. Відкритий і закритий ключі кожного учасника обміну повідомленнями в криптосистемі К8А утворюють «узгоджену пару» в тому сенсі, що вони є взаємно зворотними [2].

Алгоритм Я8А є поширеним і популярним алгоритмом, а отже його реалізацію включено до стандартних бібліотек багатьох мов програмування. При цьому, саме використання Я8А найбільш підходить для впровадження належного захисту від редагування даних з боку підприємства та співставлення отриманих даних з конкретною відповідальною за продукцію певної зміни особою. Також використання асиметричної ключової системи К8А разом з використанням хешування є основою забезпечення імітозахисіу інформації під час її надходження відкритими каналами на зберігання до контролюючих органів.

3. Дослідження використання хешування в програмі оптимізації системи контролю технологічного процесу та вибір оптимального методу для даної задачі Використання хешування для даної задачі зумовлено вимогою забезпечення імітоза- хисту (захисту від нав'язування хибних даних зловмисником під час перехоплення інформаційного повідомлення у відкритому каналі зв'язку).

В загальному випадку *хешування* (ЬазЬіп§) - це перетворення по визначеному алгоритму вхідного масиву даних довільної довжини в вихідний бітовий рядок фіксованої довжини. Хешування застосовується для побудови асоціативних масивів, пошуку дублікатів в серіях наборів даних, побудови досить унікальних ідентифікаторів для наборів даних, підрахунок контрольних сум з метою виявлення випадкових або навмисних помилок при зберіганні або передачі, для зберігання паролів в системах захисту (в цьому випадку доступ до області пам'яті, де знаходяться паролі, не дозволяє відновити сам пароль), при виробленні електронного підпису (на практиці часто підписується не саме повідомлення, а його хеш-образ), для імітозахисту тощо.

У загальному випадку однозначної відповідності між вихідними даними і хеш-кодом немає в силу того, що кількість значень хеш-функцій менше, ніж варіантів вхідного масиву; існує множина масивів з різним вмістом, але які дають однакові хеш-коди - так звані колізії, Імовірність виникнення колізій відіграє важливу роль в оцінці якості хеш-функцій.

Безпосередньо для захисту від фальсифікації переданої інформації хешування проводиться криптостійкою функцією над повідомленням, об'єднаним з ключем, відомим тільки відправнику і одержувачу повідомлення. Таким чином, криптоаналітик не зможе відновити код за перехопленим повідомленням і значенням хеш-функції, тобто, не зможе підробити повідомлення [2].

Особливістю використання хешування у якості імітозахисту для даної задачі в архіваторі системи контролю технологічного процесу є те, що у якості ключа з яким об'єднане повідомлення використовується відкритий ключ К8А, який доступний як у відповідального за продукції бригадира зміни (відправник) з одного боку, так і в контролюючих органах (одержувач) з іншого, але при цьому тримається у секреті від зловмисника. При цьому, отримане повідомлення разом з хешем використовується також для ідентифікації відправника одержувачем.

В зв'язку зі зазначеним, для забезпечення імітозахисту для даної задачі було обрано використовувати хешування МЕ>5 (Ме$$а§е Пінезі 5) - популярний 128-бітний алгоритм хешування, розроблений професором Рональдом Л. Рівестом в 1991 році. Він призначений для створення «відбитків» або «дайджестів» повідомлень довільної довжини. Прийшов на зміну МЛ4, що був недосконалим. Переваги використання цього алгоритму у вигляді насамперед доступності реалізації зумовленою популярністю та поширеністю, а також відносною швидкістю виконання, перекривають наявні недоліки, які для даної задачі не є критичними.

Висновки

Використання алгоритму К8А для забезпечення належного шифрування та алгоритму хешування М05, що використовується для організації імітозахисту через ідентифікацію користувача, створює можливості для її врахування у якості бази розробки на її основі ефективної програми оптимізації системи контролю виробничого технологічного процесу на підприємстві.

Список літератури

1. Ватолин Д. Методи сжатия данньїх. Устройст- во архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. - М.: ДИАЛОГ- МИФИ; 2003.-384 с.

2. Фергюсон Н. Практическая крптография / Н. Фергюсон, Б. Шнайер. - М.: Диалектика, 2004. -432 с.

3. Баричев С. Криптография без секретов / С. Бари- чев. -М: Горячая Линия - Телеком, 2004. - 43 с.

Надійшла до редколегії 6.05.2015

Рецензент: д-р техн. наук, проф. В.М. Рудницький, Черкаський державний технологічний університет, Черкаси.

ВЫБОР МЕТОДА ШИФРОВАНИЯ ДЛЯ ЗАДАЧИ ОПТИМИЗАЦИИ СИСТЕМЬ! ОБЬЕКТИВНОГО КОНТРОЛЯ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА

Л.А. Шувалова, С.Ю, Куницкая, И.И. Билас

Проведено исследование симметричньїх алгоритмов шифрования информации и асимметричних алгоритмов шифрований информации. На основе проведенного исследования выбран алгоритм шифрования информации для задачи оптимизации системи обьективного контроля технологического процесса. Проведено исследование использования хеширования в программе оптимизации системи контроля технологического процесса и выбор оптимального метода для данной задачи. Для обеспечения імітозащити для данной задачи вибрано использование хеширования МВ5.

Ключевьіе слова: шифрование, алгоритм шифрования, ріттографическсія система, хеширование.