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 MD5.

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 кваліметричної 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 прихування 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 AES (Advanced Encryption Standard) використовуються блоки довжиною 128 біт.

Сьогодні існує досить багато симетричних алгоритмів криптографічного захисту інформації, які широко використовуються в сучасних архіваторах. Серед них можна виділити Triple DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish, Cast-128 і деякі з AES, включаючи новий AES Rijndael поряд з ZIP-стисненням. А якщо говорити про методи шифрування, реалізовані в програмах-архіваторах, то тут вибір більш обмежений. У переважній більшості випадків в популярних архіваторах реалізований якийсь один метод. Найчастіше це ZIP-шифрування або AES Rijndael. Виняток становить PowerArchiver, в якому користувачеві надається цілих 5 варіантів кодування стислих даних: Blowfish (128 біт), DES (64 біт), Triple DES (128 біт) і Rijndael AES (128 біт) і звичайне ZIP-шифрування. Слід визнати, що стандартне ZIP-шифрування не відноситься сьогодні до числа надійних, так само як і шифрування із застосуванням алгоритму DES. Починаючи з середини 90-х років, стали з'являтися кандидати на заміну DES, найбільш відомі з яких – Triple DES, IDEA і Blowfish. Перший і останній застосовуються і сьогодні в різних програмних засобах для шифрування даних, у тому числі в архіваторах. IDEA використовується PGP (Pretty Good Privacy) і рядом інших криптографічних програм. Triple DES («потрійний DES», бо тричі шифрує інформацію «звичайним» алгоритмом DES) вільний від основного недоліку колишнього варіанта – короткого ключа. Тут ключ в 2 рази довше, і тому надійність «потрійного» DES набагато вище. Але

Triple DES успадкував і слабкі сторони свого попередника – відсутність можливостей для паралельних обчислень при шифруванні і низьку швидкість.

Сучасний 64-бітний блоковий шифр Blowfish 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 DES, Triple DES і IDEA.

Однак найбільш надійним сьогодні визнається Rijndael – новий стандарт шифрування AES. 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 AES Rijndael 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 AES [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 Elgamal (названа на честь автора, Тахіра Ельгамаля), RSA (названа на честь винахідників: Рона Рівеста, Аді Шаміра і Леонарда Адлмана), Diffie-Hellman і DSA, Digital Signature Algorithm (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 RSA стала першою системою, придатною одночасно і для шифрування, і для організації цифрового підпису. Алгоритм використовується у великому числі криптографічних додатків, включаючи PGP, S/MIME (Secure / Multipurpose Internet Mail Extensions), TLS/SSL (Transport Layer Security / Sockets Layer), IPSEC/IKE (Internet Protocol Security / Internet Key Exchange) та інших. Алгоритм RSA 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 x, то f(x) обчислити відносно просто.

2. Якщо відомо y = f(x), то для обчислення x 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 RSA використовується як *відкритий ключ* (*public key*), так і *закритий ключ* (*private key*), кожен з яких складається з пари цілих чисел. Відкритий і закритий ключі кожного учасника обміну повідомленнями в криптосистемі RSA утворюють «узгоджену пару» в тому сенсі, що вони є взаємно зворотними [2].

Алгоритм RSA є поширеним і популярним алгоритмом, а отже його реалізацію включено до стандартних бібліотек багатьох мов програмування. При цьому, саме використання RSA 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 RSA разом з використанням хешування є основою забезпечення імітозахисту 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 імітозахисту (захисту від нав'язування хибних даних зловмисником під час перехоплення інформаційного повідомлення у відкритому каналі зв'язку).

В загальному випадку *хешування* (hashing) – 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 крипостійкою 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 RSA, 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 MD5 (Message Digest 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 MD4, 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 RSA для забезпечення належного шифрування та алгоритму хешування MD5, 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. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. – М.: ДИАЛОГ-МИФИ, 2003. – 384 с.

2. Фергюсон Н. Практическая криптография / Н. Фергюсон, Б. Шнайер. – М.: Диалектика, 2004. – 432 с.

3. Баричев С. Криптография без секретов / С. Баричев. – 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 СИСТЕМЫ ОБЪЕКТИВНОГО КОНТРОЛЯ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА

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

Проведено исследование симметричных алгоритмов шифрования информации и асимметричных алгоритмов шифрования информации. На основе проведенного исследования выбран алгоритм шифрования информации для задачи оптимизации системы объективного контроля технологического процесса. Проведено исследование использования хеширования в программе оптимизации системы контроля технологического процесса и выбор оптимального метода для данной задачи. Для обеспечения імітозащиты для данной задачи выбрано использование хеширования MD5.

Ключевые слова: *шифрование, алгоритм шифрования, криптографическая система, хеширование.*

CHOICE THE ENCRYPTION METHOD FOR THE PROBLEM OF OPTIMIZATION THE SYSTEM OF OBJECTIVE CONTROL OF THE TECHNOLOGICAL PROCESS

L.A. Shuvalova, S.Y. Kunitskaya, I.I. Bilas

The study of symmetric encryption algorithms asymmetric information and encryption information. On the basis of the study the selected encryption algorithm information for the optimization problem of the system of objective control of the process. A study of the use of hashing in the program of optimization of a control system of the technological process and the choice of the optimal method for a given problem. To ensure messages to for a given task is selected using MD5 hashing.

Keywords: *encryption, encryption algorithm, cryptographic system, hashing.*