УДК 004.02

ВИКОРИСТАННЯ КРИПТОГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Лобода Ю.Г., канд. пед. наук, доцент, Орлова О.Ю., асистент
Одеська національна академія харчових технологій, м. Одеса

Вирішується завдання вибору алгоритму криптографічного захисту інформаційних ресурсів за допомогою нелінійної згортки критеріїв на основі методу аналізу ієрархій із урахуванням вимог: безпека, швидкість, характеристика алгоритму. У результаті визначено оптимальний криптоалгоритм, який забезпечує цілісність та доступність інформації.

In the paper a task of cryptographic information security algorithm choice is solving of information resources by nonlinear criteria convolution on the basis of hierarchy analysis method taking into account such requirements as safety, speed, algorithm description. As a result it was defined an optimal cryptographic algorithm, which provides integrity and availability of information.

Ключові слова: криптографічні засоби, криптоалгоритм, оптимізація вибору.

Вступ. Сучасний розвиток інформаційних технологій і, зокрема, технологій Internet/Intranet приводить до необхідності захисту інформації, що передається в рамках розподіленої корпоративної мережі, яка використовує мережі відкритого доступу. При роботі на своїх власних закритих фізичних каналах доступу ця проблема так гостро не стоїть, оскільки в цю мережу закритий доступ стороннім. Проте виділені канали може собі дозволити далеко не будь-яка компанія. Тому доводиться задовольнятися тим, що є у розпорядженні компанії. Найчастіше – це Internet. Тому потрібно винаходити способи захисту конфіденційних персональних даних, що передаються по фактично незахищеній мережі.

Із прийняттям Закону України «Про захист персональних даних» № 2297-VI від 01.06.2010 р. з'явилося нове поняття «персональні дані». До персональних даних відносяться відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [1]. Прикладами баз персональних даних можуть буди відомості про співробітників (ПІБ, паспортні дані, ІПН та інше), які обробляються бухгалтерією та відділом кадрів будь-якого підприємства або державної установи.

Мета статті полягає у розгляді питання вибору алгоритму криптографічного захисту інформаційних ресурсів за допомогою нелінійної згортки критеріїв на основі методу аналізу ієрархій із урахуванням вимог: безпека, швидкість, характеристика алгоритму. Для досягнення мети були поставлені такі завдання: визначити вимоги до алгоритмів криптографічного захисту інформаційних ресурсів; з'ясувати можливості криптоалгоритмів; визначити метод процесу оптимізації процесу вибору криптоалгоритму та його переваги/недоліки.

Матеріали і методика досліджень. Одним із напрямів захисту в інформаційних системах є криптографічний захист інформації, що передбачає використання математичних методів перетворення інформації за допомогою шифрування, вироблення імітовставки або цифрового підпису тощо. Криптографічний захист може здійснюватися у процесі передавання інформації каналами зв'язку та під час її опрацювання на робочих станціях і серверах.

До передавання інформації каналами зв'язку ставлять такі вимоги:

— забезпечення конфіденційності інформації;
— забезпечення цілісності інформації;
— автентичність сторін інформаційного обміну.

Конфіденційність інформації забезпечується симетричним (алгоритми ГОСТ 28147-89, DES, 3DES, AES, IDEA) та асиметричним (алгоритми RSA, El Gamal) шифруванням. Цілісність інформації та автентичність сторін досягається використанням хеш-функцій та технологій цифрового підпису.

Сукупність технологій, що забезпечують конфіденційність та цілісність інформації при її передаванні незахищеними каналами зв'язку, отримала назву віртуальних приватних мереж (VPN – Virtual Private Network). У процесі мережевої взаємодії захист інформації, зокрема, забезпечується за допомогою протоколів SSL, SSH, S-HTTP, IPSec тощо. Автентичність сторін інформаційного обміну досягається за рахунок використання протоколів X.509, RADIUS, TACACS+ та інших. Реалізація цих технологій може здійснюватися програмними та програмно-апаратними засобами. Захист інформації на робочих станціях і серверах може реалізовуватися за допомогою шифрування на рівні файлової системи, криптографічних

методів перевірки автентичності (цифрові сертифікати, одноразові паролі тощо), криптографічних засобів перевірки цілісності (контрольні суми).

Проблема захисту інформації через її перетворення, що унеможливлює її прочитання сторонніми особами, ще кілька десятиліть тому стосувалася в основному військових операцій або була пов'язана зі шпигунськими історіями, а не становила предмет широкого використання. Причиною бурхливого розвитку криптографії, з одного боку, є використання комп'ютерних мереж, зокрема глобальної мережі Internet, по яких передають великі обсяги інформації державного, військового, комерційного та приватного змісту, що не допускає можливості доступу до неї сторонніх осіб, а з іншого – поява нових потужних обчислювальних засобів уможливила дискредитацію низки криптографічних систем. Без криптографії не було б стільникових телефонів, банкоматів, цифрового телебачення, Internet-платежів тощо.

Методи криптографічного захисту інформації передбачають як програмне, так і апаратне використання. Програмна реалізація шифрування є дешевою та практичнішою. Водночас апаратна реалізація продуктивніша та простіша у використанні. Сучасні криптографічні системи повинні задовольняти такі загальноприйняті вимоги: вихідний текст із зашифрованого тексту можна відтворити лише за допомогою ключа дешифрування; послідовне перебирання можливих ключів дешифрування з метою відтворення вихідного тексту потребує значного часу обчислень або великих затрат на реалізацію цих обчислень; інформація про алгоритм шифрування не повинна впливати на стійкість до зламування системи шифрування; незначна зміна ключа шифрування повинна призводити до істотних змін шифрограми одного і того самого тексту.

1. Шифрування з ключем. Алгоритм шифрування з ключем поділяють на дві великі групи – алгоритми симетричного шифрування й алгоритми асиметричного шифрування.

Методи симетричного шифрування/дешифрування – це метод, за яким ключі шифрування і дешифрування є або однаковими, або легко обчислюються один із одного, забезпечуючи спільний ключ, який є таємним.

Методи асиметричного шифрування/дешифрування – набір методів криптографічного шифрування/дешифрування, в якому використовують два ключі – таємний (приватний) і відкритий; жодний із ключів не може бути обчислений з іншого за визначений час. Таке шифрування/дешифрування ще називають шифруванням/дешифруванням з відкритим ключем.

До 70-х років минулого століття застосовували лише криптографію з симетричними криптоалгоритмами. Криптографія з асиметричними криптоалгоритмами значно молодша. Симетричні та асиметричні криптоалгоритми мають переваги та недоліки. Симетричні криптоалгоритми порівняно з асиметричними мають більшу швидкодію та меншу довжину ключа. Асиметричне шифрування застосовують за такої організації криптосистем, коли використання симетричних алгоритмів є неможливим. А загалом порівнювати характеристики цих криптоалгоритмів було б некоректно: вони створені для розв'язування різних задач шифрування.

2. Метод симетричного шифрування. Симетричне шифрування ще називають шифруванням із таємним ключем, тобто з ключем, який обидва боки обміну інформацією (таємно від інших користувачів) використовують для шифрування та дешифрування повідомлень. На рис. 1 наведено структурну схему шифрування з таємним ключем. Основне призначення симетричних криптоалгоритмів – шифрування великих масивів даних із великою швидкістю. Разом із тим, через необхідність наявності захищеного каналу передавання таємного ключа ці криптоалгоритми під час створення сучасних криптосистем виявляють дуже низьку гнучкість. Розрізняють дві великі групи алгоритмів симетричного шифрування: потокове шифрування та блокове шифрування.

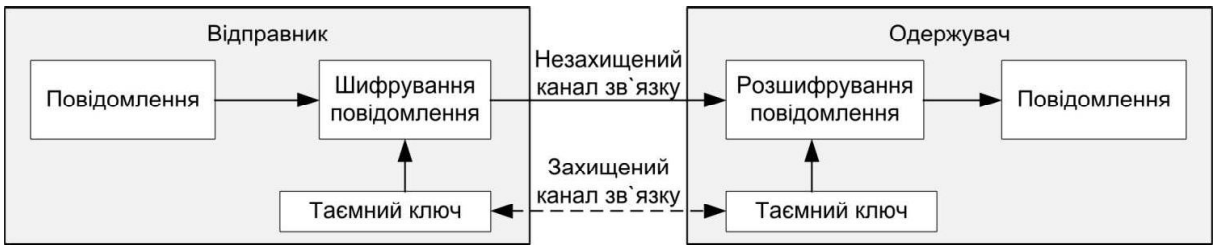

Рис. 1 – Структурна схема шифрування з таємним ключем

3. Метод асиметричного шифрування. Проблему зростання обсягів шифрованої інформації у криптографії вирішують підвищенням швидкодії традиційних методів шифрування з таємним ключем. Проте застосування цих методів в умовах постійного зростання кількості учасників спільної роботи (децентралізована структура управління) й ускладнення організації взаємодії між ними, зокрема попарного обміну інформацією, виявляється неефективним. Це зумовлено тим, що зі збільшенням кількості учасників об-

міну інформацією квадратично зростає кількість таємних ключів. Можна показати, що для N учасників кількість таємних ключів у такій системі сягає $N(N-1)/2$. Крім того, у методах симетричної криптографії з таємним ключем ускладнене довірене узгодження таємного ключа. Із метою зменшення цих недоліків було розроблено методи асиметричного шифрування з відкритим ключем. Шифрування з відкритим ключем – порівняно нова галузь криптографії. В асиметричних криптоалгоритмах для шифрування і дешифрування використовують різні ключі: для шифрування – відкриті, для дешифрування – таємні. Асиметрична криптографія основана на ідеях В. Діффі та М. Хеллмана про шифрування з двома ключами, що стали відомими у 1976 році. Але першим алгоритмом асиметричного шифрування, що набув практичного значення, став алгоритм, який запропонували Р. Рівест, А. Шамір і Л. Адлеман у 1978 році. Він дістав назву алгоритм RSA. На рис. 2 наведено структурну схему шифрування з відкритим ключем.

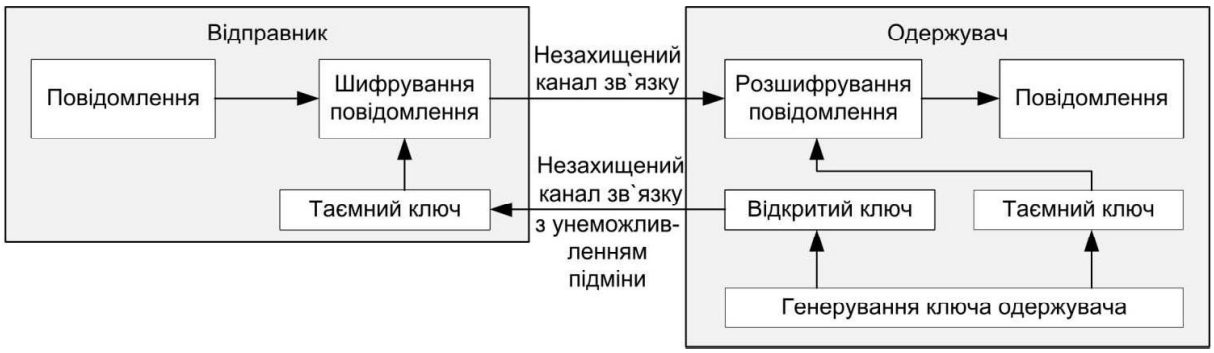

Рис. 2 – Структурна схема шифрування з відкритим ключем

Математичним обґрунтуванням асиметричних криптоалгоритмів є важко оборотні (односторонні) функції. У теорії складності обчислень розглядають поняття, яке характеризує рівень складності обчислень (кількість операцій) залежно від розміру вхідних даних. Поширеними є поліноміальний та експоненційний характери залежності складності обчислень від кількості вхідних даних. В асиметричній криптографії В. Діффі та М. Хеллмана зашифроване повідомлення за наявності таємного ключа дешифровується за поліноміальний час роботи обчислювальної системи, а в разі його відсутності – за експоненційний час. Сучасна асиметрична криптографія гоунтується на алгоритмах Ель-Гамаля та Міллера–Коблиця. Теоретичну основу стійкості алгоритму RSA становить проблема факторизації великих цілих чисел, а алгоритмів Ель-Гамаля та Міллера–Коблиця – проблема дискретного логарифмування. Сьогодні відомі численні вразливості цих алгоритмів. Алгоритми шифрування на відкритому ключі замінили стійкіші алгоритми шифрування на еліптичних кривих, які запропонували окремо В. Міллер і Н. Коблиць у 1986 р. [2].

Алгоритми асиметричного шифрування, так само, як і симетричного, застосовують для шифрування масивів даних, але їхня швидкість значно нижча. Основне призначення асиметричних алгоритмів – забезпечення ефективного функціонування сучасних криптосистем. Саме ці алгоритми покладено в основу задач автентифікації користувачів, контролю цілісності та доступності інформації, унеможливлення відмови від авторства чи факту одержання даних тощо, зокрема, в організації електронного урядування. Найповніше ці вимоги задовольняють такі алгоритми асиметричного шифрування: Mars, RC6, Rijndael, Serpent, Twofish (табл. 1).

Таблиця 1 – Вибрані для порівняння алгоритми асиметричного шифрування

Алгоритм	Розробник	Країна	Швидкодія (asm, 200М Гц)
MARS	IBM	US	8 Мбайт/с
RC6	R.Rivest & Co	US	12 Мбайт/с
Rijndael	V.Rijmen & J.Daemen	BE	7 Мбайт/с
Serpent	Universities	IS, UK, NO	2 Мбайт/с
TwoFish	B.Schneier & Co	US	11 Мбайт/с

Важливого практичного значення асиметричні криптоалгоритми набули у застосуванні систем електронно-цифрового підпису (ЕЦП). ЕЦП – цифрова послідовність, що додається до повідомлення для забезпечення цілісності інформації та підтвердження авторства і формується із застосуванням асиметричних криптосистем. У ЕЦП для формування підписаних повідомлень використовують таємний ключ, а для перевірки підпису – відкритий.

У процесі захисту інформаційних ресурсів виникає проблема оптимального вибору алгоритму криптографічного захисту інформації. Кожен із великої кількості криптографічних алгоритмів має певні пере-

ваги та недоліки. Тому обсяг аналізу інформації щодо оцінення і вибору криптографічного алгоритму, який найкраще задовольняє вимоги захисту інформації, є доволі великим. Процес вибору передбачає кількісний та якісний аналіз у процесі порівняння різних альтернатив. Зі зростанням кількості критеріїв порівняння та кількості альтернатив, які можуть істотно впливати на кінцевий результат, людині зробити вибір серед такої множини варіантів досить складно [3]. Саме тому виникає необхідність використання систем підтримки прийняття рішення, що дає змогу на основі експертних оцінок оптимізувати вибір алгоритму криптографічного захисту інформації, а також не тільки виконувати якісний, кількісний аналіз, враховуючи найважливіші вимоги до алгоритмів, але і науково обгрунтувати вибір [4].

Для захисту інформаційних ресурсів визначальними є такі критерії порівняння: надійне виконання алгоритму як в апаратному, так і програмному виконанні; швидке генерування та узгодження ключів, їх використання; мінімальне використання оперативної пам'яті; стійкість до атак; гнучкість; висока пропускна здатність. Отже, визначимо основні критерії порівняння алгоритмів криптографічного захисту інформації: безпека; швидкість; загальні параметри алгоритму.

Критерій «безпека» є найважливішим чинником під час оцінювання і порівняння таких можливостей, як стійкість алгоритму до криптоаналізу, дослідження його математичної основи, випадковість вихідних значень алгоритму і відносна безпека порівняно з іншими алгоритмами.

Критерій «швидкість» є наступним важливим критерієм оцінювання, який характеризує обчислювальну ефективність на різних платформах, вимоги пам'яті, час, затрачений на шифрування та дешифрування, швидкість реагування на атаки.

Загальні параметри алгоритму. Третім пріоритетним критерієм оцінки алгоритмів є характеристика алгоритму, під якою розуміють: гнучкість, технічні засоби, придатність програмного забезпечення і простоту алгоритму. Гнучкість означає здатність алгоритму до:

— управління ключем, зведення розмірів до мінімуму;
— безпечного й ефективного функціонування в різних типах програмного середовища;
— здійснення хешування алгоритму, можливість забезпечення додаткових криптографічних послуг.

Виконання цих вимог необхідне для того, щоб технічні засоби і програмне забезпечення підтримували реалізацію вибраного криптоалгоритму. В табл. 2 наведено порівняльну характеристику п'яти криптоалгоритмів за визначеними критеріями порівняння [5].

Таблиця 2 – Порівняльна характеристика п'яти криптоалгоритмів

Категорія	Serpent	Twofish	MARS	RC6	Rijndael
Криптостійкість	+	+	+	+	+
Запас криптостійкості	++	++	++	+	+
Швидкість шифрування при програмній реалізації	-	+-	+-	+	+
Захист від атак під час виконання і використання потужності	+	+-	-	-	+
Захист від атак за необхідної потужності на процедуру розширення ключа	+-	+-	+-	+-	-
Захист від атак за використовуваної потужності для реалізації у смарт-картах	+-	+	-	+-	+
Можливість паралельних обчислень	+–	+–	+–	+–	+
Можливість розширення ключа «на льоту»	+	+	+–	+–	+–

Криптостійкість алгоритмів є достатньою – під час досліджень не було виявлено жодних атак, що реально реалізовувалися, на повноцінних версіях алгоритмів. У цьому випадку криптоаналітики, зазвичай, досліджують варіанти алгоритмів із усіченою кількістю раундів, або з деякими внесеними змінами, незначними, але які послаблюють характеристики алгоритму. Під запасом криптостійкості розуміють співвідношення повної (передбаченої в специфікаціях алгоритмів) кількості раундів і максимального з тих варіантів, проти яких діють будь-які криптоаналітичні атаки. Наприклад, за допомогою диференціально-лінійного криптоаналізу розкривається 11-раундовий Serpent, тоді як в оригінальному алгоритмі виконуються 32 раунди.

Висновки. Запас криптостійкості у Rijndael і RC6 дещо нижчий, ніж у решти алгоритмів. З характеристики алгоритмів видно, що всі вони підтримують розширення ключа «на льоту» (тобто підключі можуть генеруватися безпосередньо у процесі шифрування – за необхідністю), проте тільки Serpent і Twofish підтримують таку можливість без будь-яких обмежень.

Під наявністю варіантів реалізації (гнучкість) ідеться про можливість по-різному реалізовувати будь-які операції алгоритму з оптимізацією під конкретні цілі. Найпоказовішими в цьому сенсі є згадані рані-

ше варіанти процедури розширення ключа алгоритму Twofish, що дають змогу оптимізувати реалізацію алгоритму залежно, передусім, від частоти зміни ключа до критеріїв оцінки алгоритмів криптографічного захисту інформації для застосування в електронному урядуванні рекомендується вибирати алгоритм, який за інтегральним показником є найефективнішим.

Критерій «безпека» має найбільший пріоритет і здійснює найбільший вплив на отримані результати, а критерії «швидкість» і «характеристика алгоритму» є вторинними щодо «безпеки». Керуючись необхідністю забезпечення надійної безпеки алгоритмів від атак, можна сказати, що щодо безпеки MARS, Serpent і Twofish мають високий рівень захисту, але RC6 і Rijndael мають вищий і надійніший захист. RC6 і Rijndael загалом демонструють швидкість шифрування і дешифрування, вищу за середню для 128-бітних ключів, але щодо 32-бітних платформ RC6 має найбільшу швидкість. MARS має середню швидкість виконання цих дій. Для Twofish час, затрачений на шифрування і дешифрування, відрізняється, але в обох випадках рівень є вищим за середній. Serpent показав найнижчий показник порівняно з іншими алгоритмами.

Rijndael потребує невеликих затрат оперативної пам'яті і відповідно є найкращим за обмежених можливостей. Serpent також забезпечує належний рівень шифрування та дешифрування за малої оперативної пам'яті. RC6 має невелику оперативну пам'ять, що є позитивним в обмеженому просторі, але має недолік при безперервній здатності обчислення підключів для дешифрування – високу вимогу до оперативної пам'яті щодо інших алгоритмів. MARS не задовольняє вимоги за обмеженого середовища та вимагає додаткових ресурсів.

Serpent і Rijndael мають найкращу апаратну продуктивність для обох способів зворотного і незворотного зв'язку. Serpent має найвищу продуктивність у незворотному зв'язку, Rijndael пропонує найкращу ефективність роботи у зворотному зв'язку. RC6 і Twofish мають середню продуктивність, і обидва алгоритми можуть виконуватись компактно. MARS має високі вимоги і загалом його продуктивність є нижчею від середнього рівня. Під час атак на виконання добре себе проявили алгоритми Rijndael і Serpent, швидко виявляючи і запобігаючи їм. Довше і з більшою складністю виконує Twofish, а RC6 і MARS з найбільшою затратою часу і труднощам протидіють атакам. Twofish, MARS і RC6 потребують мало додаткового простору, щоб здійснювати шифрування та дешифрування. Хоч Rijndael у цьому аспекті поступається за швидкістю, але може розділяти деякі технічні засоби.

Twofish підтримує безперервне обчислення, підрахунок підключів як для шифрування, так і для дешифрування. Serpent також підтримує безперервний підрахунок підключів як для шифрування, так і для дешифрування, проте процес дешифрування вимагає одного додаткового обчислення підрахунку. Алгоритм Rijndael підтримує безперервне обчислення підключів для шифрування, але вимагає попереднього одноразового виконання повного ключового списку до ранішого дешифрування зі специфічним ключем. MARS має особливі характеристики, які є схожими до Rijndael, але додатково навантажує ресурс на MARS виконання. RC6 підтримує безперервне обчислення підключів тільки для шифрування. Кожен із алгоритмів забезпечує надійну захищеність і має певні переваги у деяких галузях порівняно з іншими. Методом аналізу ієрархій на основі нелінійної згортки критеріїв було досліджено і математично обґрунтовано вибір алгоритму Rijndael як такий, що найкраще задовольняє вимоги захисту інформації.

Література

1. Верховна Рада України; Закон від 01.06.2010 № 2297-VI Про захист персональних даних (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481). – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2297-17.
2. Грайворонський М.В. Безпека інформаційно-комунікаційних систем [Текст] / М.В. Грайворонський, О.М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с.
3. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C (second Edition) [Text] / B. Schneier. – N.Y.: John Wiley & Sons, Inc., 1996. – 758 p.
4. Ногин В. Д. Принятие решении в многокритериальной среде: количественный подход [Текст] / В.Д. Ногин. – М. : Физматлит, 2002. – 144 с.
5. Алгоритмы симметричного шифрования. Ч.3. Разработка Advanced Encryption Standart (AES) [Електронний ресурс]. – Режим доступу: http://www.intuit.ru/department/security/networksec/4/5.html.