УДК 004.056

ВИКОРИСТАННЯ МЕТОДІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

М.В. ЗАХАРОВА, Т.С. ПІСКУНОВА, С.В. ШПАРА

Київський національний університет технологій та дизайну

У цій роботі проведено дослідження можливості ефективного використання методів криптографічного захисту інформації від несанкціонованого доступу. Запропонований підхід дозволяє зробити вибір методу захисту на основі обраних критеріїв ефективності, а також оцінити можливість практичного використання розглянутих криптографічних методів захисту.

Тенденцією, що характеризує розвиток сучасних інформаційних технологій є зростання числа комп‘ютерних злочинів пов‘язаних з несанкціонованим доступом до збереженої або переданої інформації. На сьогоднішній день для захисту інформації широко застосовуються криптографічні методи захисту інформації. При організації захисту інформації методом шифрування з використанням ключів застосовуються два різновиди алгоритмів шифрування – симетричні та з відкритим ключем. Симетричні алгоритми шифрування (або криптографія з секретним ключем) основані на тому, що відправник і одержувач інформації використовують один і той же ключ. Цей ключ повинен зберігатися в таємниці і передаватися способом, що виключає його перехоплення. Зазвичай ключ шифрування є файлом або масивом даних і зберігається на персональному ключовому носієві [2]. У асиметричних алгоритмах шифрування (або криптографії з відкритим ключем) для шифрування інформації використовують один ключ (відкритий), а для розшифрування інший (секретний). Ці ключі різні і не можуть бути отримані один з іншого. Розділення на симетричні алгоритми і алгоритми з відкритим ключем виникло у зв'язку з винаходом нових засобів, у тому числі і математичних, таких, що дають можливість захищатися методами криптографії не лише від загрози розкриття інформації, але і від багатьох інших загроз, пов‘язаних з несанкціонованим доступом [4].

Об’єкти та методи дослідження

При практичному використанні криптографічних методів необхідно враховувати особливості конкретної системи захисту інформації, її функції і умови експлуатації. Не дивлячись на існування добре відомих криптоалгоритмів (як з симетричними, так і несиметричними ключами), криптостійкість яких або доведена математично, або основана на необхідності вирішення математично складного завдання (факторизації, дискретного логарифмування і тому подібне) існує проблема забезпечення надійності криптосистеми. Основними причинами ненадійності криптографічних систем є використання нестійких алгоритмів, неправильна реалізація або використання методів криптографічного захисту.

Постановка завдання

У даній роботі проводиться дослідження можливості ефективного використання методів криптографічного захисту інформації від несанкціонованого доступу. При аналізі сильних і слабких сторін криптографічних методів захисту необхідно зробити вибір методу захисту на основі обраних критеріїв ефективності, а також оцінити можливість практичного використання розглянутих криптографічних методів захисту.

Результати та їх обговорення

Основні методи криптографічного захисту інформації можуть бути класифіковані різним чином, але найчастіше вони підрозділяються залежно від кількості ключів, що використовуються у відповідних криптоалгоритмах. Розглянемо симетричні та асиметричні криптоалгоритми. Симетричним називають криптографічний алгоритм, в якому ключ, що використовується для шифрування повідомлень, може бути отриманий з ключа розшифрування і навпаки [2]. У симетричних алгоритмах законний користувач Р за допомогою деякого шифратора $Ш_К$ перетворить послідовність $X = (x_1,...,x_n)$, яка називається відкритою інформацією, в шифровану інформацію $Y = Ш_к(x)$ (рис. 1). Алгоритм роботи шифратора $Ш_к$ залежить від параметра $К = К_х$ (ключа), відомого користувачеві. Законні користувачі, яким призначена інформація X, здійснюють розшифрування інформації також за допомогою деякого алгоритму, залежного від параметра $K^/$, пов'язаного з K. Зазвичай $K^/ = K$. У даному випадку кожен законний користувач спочатку володіє як перетворенням $Ш_к$, так і перетворенням $Ш_к^{-1}$ – зворотним до $Ш_к$, тоді як незаконний користувач не має ключа K, тобто не повністю знає перетворення $Ш_к$ і $Ш_к^{-1}$ [4].

Рис. 1. **Схематичне відображення моделі симетричної системи**

Симетричні криптосистеми засновані на потокових і блокових алгоритмах шифрування. У потокових алгоритмах кожен біт відкритого тексту зашифровується (і розшифровується) шляхом додавання по модулю 2 з бітом псевдовипадкової послідовності – гамми, незалежно від інших бітів. Таким чином, перетворення кожного символу відкритого тексту міняється від одного символу до іншого [5]. Стійкість потокових алгоритмів шифрування залежить від того, наскільки вироблена гамма володіє властивістю рівновипадковості появи чергового символу.

Перевагами потокових алгоритмів є висока швидкість шифрування, відносна простота, відсутність в ньому розмноження помилок. Недоліками є: гамму недопустимо використовувати більше одного разу (з точки зору безпеки), необхідність підпорядкування вимозі синхронності виконання операцій шифратором на приймачі та передавачі, яка виражається в передачі синхронізуючої випадкової послідовності перед заголовком повідомлення, до його розшифрування (так званий псевдовипадковий додатковий ключ, який використовується для модифікації ключа шифрування для поліпшення криптостійкости).

Для блокових алгоритмів шифрування відкритий текст спочатку розбивається на рівні по довжині блоки, а потім шифрується в рамках кожного блоку функцією, залежною від ключа, в блок шифртекста тієї ж довжини [5]. У разі коли довжина відкритого тексту некратна довжині вхідних блоків

в алгоритмі шифрування, застосовується операція доповнення останнього блоку відкритого тексту до необхідної довжини. Суть алгоритмів блокового шифрування полягає в багатократному застосуванні до блоку відкритого тексту математичного перетворення з тим, аби створити залежність кожного біта шифртекста від кожного біта ключа і відкритого тексту. Блоковий алгоритм має бути сконструйований так, щоб зміна навіть одного біта відкритого тексту або ключа привоздила б до зміни приблизно 50 % бітів шифрованого тексту, при цьому жоден біт відкритого тексту ніколи не повинен прямо вводитися в шифртекст [3]. Перетворення, що базуються на даних алгоритмах, розділяють на складні (це звичайно нелінійні операції) і прості (у основі яких лежить перемішування), причому конструкція перших забезпечує криптостійкість систем. Найбільш поширені алгоритми блокового шифрування:

– режим простої заміни або режим кодової книги (ідентичні блоки відкритого тексту шифруються однаковим чином на одному і тому ж ключі);

– режим гамування (початковий стан вихідної гамми задається синхронним посиланням з каналу зв'язку, отримана гамма проходить обробку через алгоритм блокового шифрування і потім підсумовується по модулю 2 з блоком відкритого тексту);

– режим гамування із зворотним зв'язком по виходу (при тому ж синхронному посиланні і наявності зворотного зв'язку по шифртексту гамувааня здійснюється перед тим, як результуючий блок буде перетворений алгоритмом блокового шифрування).

Перевагами алгоритмів блокового шифрування (окрім режиму простої заміни) є:

– кожен біт шифртекста залежить від всіх бітів блоку відкритого тексту і жодні два блоки відкритого тексту не представляються одним і тим же блоком шифртекста;

– Можливість вживання таких алгоритмів для виявлення маніпуляцій з повідомленнями, які створюються активними перехоплювачами.

При цьому використовуються факт розмноження помилок в шифрах і здатність систем легко генерувати код аутентифікації повідомлень.

Недоліками алгоритмів блокового шифрування є:

– піддаються обмеженому криптоаналізу «з словником»;

– пов'язані з розмноженням помилок (оскільки один помилковий біт при передачі може викликати ряд помилок в розшифрованому тексті);

– розробка і реалізація складніші, ніж в систем потокового шифрування.

На практиці для шифрування довгих повідомлень застосовуються потокові алгоритми або блокові алгоритми із зворотними зв'язками. Багатократне чергування простих перестановок і підстановок, керованих досить довгим секретним ключем, дозволяє отримати досить стійкий блоковий алгоритм з хорошим розсіюванням і перемішуванням [3]. Як найбільш популярні на сьогоднішній день симетричні алгоритми шифрування можна виділити DES, IDEA, ГОСТ 28147–89, Triple, RC2, RC5, BLOWFISH та інші.

Кожен алгоритм оцінюється за наступними критеріями: розміри вхідного і вихідного блоків; розмір ключа; складність алгоритму перетворення даних; швидкість перетворення даних та стійкість до

криптоатак. Стійкість і швидкість перетворення даних оцінювалися за 6–бальною шкалою (6–мінімальна, 1–максимальна оцінка) [1] (табл.1).

Таблиця 1. **Результати порівняння алгоритмів**

Алгоритм	Розмір вхідного блоку, біт	Розмір вихідного блоку, біт	Розмір ключа, біт	К-сть циклів перетворень в алгоритмі	Стійкість алгоритму	Швидкість перетворень
DES	64	64	56	16	3	5
IDEA	64	64	128	12	5	2
ГОСТ 28147–89	64	64	256	32	1	6
BLOWFISH	64	64	448	16	2	3
FEAL	64	64	64	від 4 до 32	4	4
RC5	32 або 64 або 128	32 або 64 або 128	від 0 до 2040	від 0 до 255	6	1

Стійкість алгоритмів шифрування розглядалася за наступними критеріями: розмір ключа; складність перетворення даних; час існування алгоритму.

З точки зору криптоаналізу важливу роль грає час існування алгоритму. Якщо алгоритм використовується тривалий час, він стає привабливою метою для криптоаналітиків [3] і на розкриття такого алгоритму шифрування можуть бути виділені великі обчислювальні ресурси. Відомим прикладом даного алгоритму може виступати алгоритм DES.

Згідно таблиці 1 найбільш стійким до криптоатак противника є алгоритм шифрування ГОСТ 28147–89, проте він є найповільнішим серед розглянутих.

У сучасних інформаційних системах симетричні методи шифрування можуть застосовуватися з метою не допустити несанкціонований доступ до інформації у відсутність власника. Це може бути як архівне шифрування вибраних файлів, так і автоматичне шифрування цілих логічних і фізичних дисків. Симетричні алгоритми також використовуються для захисту даних, які передаються по відкритих каналах зв'язку. [5]

Суть систем з відкритим ключем або асиметричних криптосистем в тому, що кожним адресатом генеруються два ключі, зв'язані між собою за певним правилом [4]. Для шифрування даних використовується один ключ, для розшифрування – другий. Кожен з кореспондентів системи володіє ключем $k = (k_з, k_p)$, що складається з відкритого ключа $k_з$ і секретного ключа k_p. Відкритий ключ визначає правило шифрування $\mathrm{E_k}$, секретний ключ – правило розшифрування D_k. Ці правила зв'язані співвідношенням:

$$D_k(E_r(X)) = Y.$$

Для будь-якого відкритого тексту X і будь-якого зашифрованого тексту Y. Знання відкритого ключа не дозволяє за прийнятний час (або з прийнятною складністю) визначити секретний ключ. Позначимо правила шифрування і розшифрування (на обраному ключі k) довільного кореспондента А

символами E_A і D_A відповідно. Кореспондент В, бажаючи відправити конфіденційне повідомлення X кореспондента А, отримує копію E_A, обчислює шифртекст $Y = E_A(X)$, який направляє по каналу зв'язку кореспондентові А. кореспондент В, отримавши повідомлення Y, застосовує до нього перетворення D_A, отримуючи відкритий текст X.

Криптографічні системи з відкритим ключем використовують безповоротні або однобічні функції, які володіють наступними властивостями: при заданому значенні X відносно просто обчислити значення $f(x)$, проте якщо $y = f(x)$, то немає простого шляху для обчислення значення X. Іншими словами, надзвичайно важко розрахувати значення зворотної функції $f^{-1}(y)$ [3]. Дослідження безповоротних функцій проводилося в основному по трьох напрямах: дискретне піднесення до степеня; множення простих чисел; комбінаторні завдання, зокрема завдання про укладання ранця.

Порівняння асиметричних криптосистем проводиться за наступними критеріями: швидкість роботи алгоритмів і використовувані математичні перетворення інформації. Швидкість перетворення даних оцінювалася за 5–бальною шкалою (1–максимальна, 5–мінімальна оцінка). Результати порівняння асиметричних методів шифрування приведені в табл. 2.

Таблиця 2. **Результати порівняння асиметричних методів шифрування**

Алгоритм	Перетворення	Швидкість роботи
RSA	Дискретне піднесення до степеня, розкладання числа на множники	5
Диффи-Хеллмана	Дискретне піднесення до степеня	2
Эль-Гамаля	Дискретне піднесення до степеня	3
Месси-Омуры	Дискретне піднесення до степеня	4
Ранцевая система	Задача укладання ранця	1

Найстійкішим з існуючих алгоритмів вважається RSA, тому що лише один раз вдалося розкрити шифр RSA для 500-значного ключа. Для цих цілей було задіяно 1600 комп'ютерів добровольців впродовж 5 місяців безперервної роботи [1]. Слід зазначити, що при використанні системи RSA з ключами завдовжки 512–1024 біт зламати шифри буде практично неможливо. Проте, система RSA працює в тисячу разів повільніше за алгоритм DES і вимагає, аби ключі були приблизно в 10 разів довше. Хоча вочевидь, що використання систем з відкритим ключем може бути обмежене завданням обміну ключами з подальшим їх вживанням в симетричній криптографії, тобто використання так званих гібридних систем [4]. Результати порівняння класичного криптографічного алгоритму DES і криптографічного алгоритму з відкритим ключем RSA приведені в табл. 3.

Таблиця 3. **Результати порівняння DES та RSA**

Характеристика	DES	RSA
Швидкість роботи	Швидка	Повільна
Використовувана функція	Перестановка й підстановка	Піднесення до степеня
Довжина ключа	56 біт	300…600 біт
Найменш витратний криптоаналіз	Перебір по всьому ключовому простору	Розкладання модуля
Часові затрати на криптоаналіз	Сторіччя	Залежать від довжини ключа
Час генерації ключа	Мілісекунди	Десятки секунд
Тип ключа	Симетричний	Асиметричний

При аналізі слабких і сильних сторін симетричних і асиметричних систем визначено, що асиметричні системи шифрування забезпечують значно менше швидкості шифрування, чим симетричні через що їх зазвичай використовують не стільки для шифрування повідомлень, скільки для шифрування ключів, що пересилаються між кореспондентами, які потім використовуються в симетричних системах. Головною перевагою криптосистем з відкритим ключем є їх потенційно висока безпека: немає необхідності ні передавати, ні повідомляти кого б то не було значення секретних ключів, ні переконуватися в їх достовірності. У симетричних криптосистемах існує небезпека розкриття секретного ключа під час передачі.

Проте, алгоритми, які лежать в основі криптосистем з відкритим ключем, мають наступні недоліки:

– Генерація нових секретних і відкритих ключів заснована на генерації нових великих простих чисел, а перевірка простоти чисел займає багато машинного часу;

– Процедури шифрування і розшифрування, пов'язані з піднесенням до ступеня багатозначного числа, досить громіздкі.

Тому швидкодія криптосистем з відкритим ключем зазвичай в сотні і більше разів менше швидкодії симетричних криптосистем з секретним ключем.

Алгоритми асиметричного шифрування застосовуються для вирішення багатьох завдань: аутентифікація користувачів і повідомлень, генерація сеансових ключів в інформаційних системах, для систем пізнання «свій-чужий».

Висновки

В результаті проведених досліджень можливості ефективного використання методів криптографічного захисту інформації від несанкціонованого доступу можна зробити висновок, що в сучасних інформаційних системах для шифрування повідомлень, які передаються, використовують симетричні алгоритми шифрування, а асиметричні алгоритми, зважаючи на їх велику обчислювальну

складність, застосовують для генерації і поширення сеансових ключів. Усунути основні недоліки, властиві обом методам, дозволяє комбіноване використання симетричного і асиметричного шифрування. При комбінованому методі шифрування зберігаються переваги високої секретності, що надаються асиметричними криптосистемами з відкритим ключем, і переваги високої швидкості роботи, властиві симетричним криптосистемам з секретним ключем. Запропонований підхід дозволяє зробити вибір методу захисту на основі обраних критеріїв ефективності, а також оцінити можливість практичного використання розглянутих криптографічних методів захисту.

ЛІТЕРАТУРА

1. Гнєздов Г.Г. Сучасні методи криптографічного захисту інформації. –К.: 2002 – 31 с.
2. Ключевський Б.Ю. Захист інформації: комп'ютерна криптографія. –М.: Гротек, 1998 – 62 с.
3. Рублінецький В.І. Введення в комп'ютерну криптологію. Харків: ОКО, 1997 – 125 с.
4. Сидельніков Ст.М., Відкрите шифрування на основі двійкових код Ріда – Маллера, Дискретна математика, 1994, т. 6, випуск 2, с. 3–20.
5. Чижухін Г.Н. Основи захисту інформації в обчислювальних системах і мережах ЕОМ. Пенза, 2001 – 164 с.